ESET CYBER SECURITY PRO

pour Mac

Manuel d'installation et guide de l'utilisateur

Cliquez ici pour télécharger la version la plus récente de ce document



ESET CYBER SECURITY PRO

Copyright © 2013 **ESET, spol. s r.o.**
ESET Cyber Security Pro a été développé par ESET, spol. s r.o.
Pour plus d'informations, visitez www.eset.com.
Tous droits réservés. Aucune partie de cette documentation ne peut être reproduite, stockée dans un système d'archivage ou transmise sous quelque forme ou par quelque moyen que ce soit, électronique, mécanique, photocopie, enregistrement, numérisation ou autre, sans l'autorisation écrite de l'auteur.
ESET, spol. s r.o. se réserve le droit de modifier les applications décrites sans préavis.

Service client : www.eset.com/support

RÉV. 11. 1. 2013

Sommaire

1. ESET Cyber Security Pro

ESET Cyber Security Pro représente une nouvelle approche d'une sécurité véritablement intégrée de l'ordinateur. La version la plus récente du moteur d'analyse ThreatSense®, alliée à la protection du client de messagerie, au pare-feu personnel et au contrôle parental, combine rapidité et précision pour sécuriser votre ordinateur. Cette combinaison produit un système intelligent qui est constamment à l'affût des attaques et des logiciels malveillants susceptibles de mettre en danger votre ordinateur.

ESET Cyber Security Pro est une solution complète de sécurité qui résulte de notre engagement à long terme d'offrir à la fois une protection maximale et un impact minimal sur le système. Nos technologies avancées, basées sur l'intelligence artificielle, permettent une élimination proactive des infiltrations de virus, vers, chevaux de Troie, spyware, logiciels publicitaires, rootkits et autres attaques basées sur Internet sans handicaper les performances du système ni interrompre le fonctionnement de votre ordinateur.

1.1 Nouveautés

Pare-feu
Le pare-feu personnel contrôle tout le trafic réseau entrant et sortant sur le système. Pour ce faire, il autorise ou refuse les connexions réseau individuelles en fonction de règles de filtrage spécifiées. Il offre une protection contre les attaques provenant d'ordinateurs distants et permet de bloquer certains services.

Contrôle parental
Le contrôle parental permet de bloquer des sites susceptibles de contenir du matériel potentiellement offensant. Les parents peuvent interdire l'accès à 27 catégories de sites Web prédéfinies. Cet outil permet d'empêcher les enfants et les adolescents d'accéder à des pages présentant du contenu inapproprié ou préjudiciable.

Protection du client de messagerie
La protection de la messagerie permet de contrôler la communication par courrier électronique effectuée via les protocoles POP3 et IMAP.

Analyse des supports amovibles
ESET Cyber Security Pro offre une analyse à la demande du support amovible introduit (CD, DVD, USB, périphérique iOS, etc.).

Joignez le réseau ESET Live Grid
Basé sur le système d'alerte anticipée ThreatSense.NET, ESET Live Grid est conçu pour offrir des niveaux de sécurité supplémentaires à votre ordinateur. Il surveille en permanence les programmes et processus en cours sur votre système à la lumière des renseignements les plus récents collectés auprès de millions d'utilisateurs d'ESET à travers le monde. Qui plus est, les analyses de votre système sont plus rapides et plus précises, car la base de données ESET Live Grid grandit avec le temps. Cela nous permet d'offrir aux utilisateurs une meilleure protection proactive et une analyse plus rapide. Nous recommandons d'activer cette fonctionnalité et vous remercions pour votre soutien.

Nouveau design
La fenêtre principale de ESET Cyber Security Pro a été entièrement remodelée et les paramètres avancés (Préférences) sont désormais plus intuitifs afin de faciliter la navigation.

1.2 Configuration système

Pour garantir le fonctionnement correct de ESET Cyber Security Pro, le système doit répondre à la configuration suivante :

	Configuration système
Architecture du processeur	Intel® 32 bits, 64 bits
Système d'exploitation	Mac OS X version 10.6 et ultérieure
Mémoire	300 Mo
Espace disque disponible	150 Mo

2. Installation

Avant de commencer l'installation, fermez tous les programmes ouverts sur votre ordinateur. ESET Cyber Security Pro contient des composants qui peuvent entrer en conflit avec les autres programmes antivirus qui sont peut-être installés sur votre ordinateur. ESET recommande vivement de supprimer les autres programmes antivirus afin d'éviter tout problème éventuel.

Pour lancer l'assistant d'installation, effectuez l'une des opérations suivantes :

- Si vous effectuez l'installation à partir du CD/DVD d'installation, installez-le dans le lecteur, ouvrez-le à partir du Bureau ou depuis le **Finder**, puis double-cliquez sur l'icône **Installer**.
- Si vous effectuez l'installation à partir d'un fichier que vous avez téléchargé sur le site ESET, ouvrez ce fichier et double-cliquez sur l'icône **Installer**.



Lancez le programme d'installation ; l'assistant d'installation vous guidera dans les opérations de configuration de base. Pendant la première phase de l'installation, le programme d'installation recherchera automatiquement la dernière version du produit en ligne. S'il la trouve, le programme d'installation proposera de la télécharger et lancera le processus d'installation.

Après avoir accepté les termes du contrat de licence de l'utilisateur final, vous pouvez choisir les modes d'installations suivants :

- Installation standard 5
- Installation personnalisée 5

2.1 Installation standard

Le mode d'installation standard comprend des options de configuration qui correspondent à la plupart des utilisateurs. Ces paramètres offrent une sécurité maximale tout en permettant de conserver d'excellentes performances système. L'installation standard est l'option par défaut qui est recommandée si vous n'avez pas d'exigence particulière pour certains paramètres.

Live Grid
Le système d'alerte anticipé Live Grid veille à ce qu'ESET soit immédiatement et continuellement informé des nouvelles infiltrations afin de protéger rapidement nos clients. Ce système permet de soumettre de nouvelles menaces au laboratoire d'ESET, où elles sont analysées, traitées et ajoutées à la base des signatures de virus. Par défaut, l'option **Activer le système d'alerte anticipé Live Grid** est sélectionnée. Cliquez sur **Configuration...** pour modifier les paramètres détaillés de soumission des fichiers suspects. Pour plus d'informations, reportez-vous à la section Live Grid 21.

Applications spéciales
La dernière étape de l'installation consiste à configurer la détection des **applications potentiellement indésirables**. De tels programmes ne sont pas nécessairement malveillants, mais peuvent avoir une incidence négative sur le comportement du système d'exploitation. Ces applications sont souvent associées à d'autres programmes et peuvent être difficiles à remarquer lors de l'installation. Ces applications affichent habituellement une notification pendant l'installation, mais elles peuvent facilement s'installer sans votre consentement.

Après l'installation de ESET Cyber Security Pro, vous devez effectuer une analyse de l'ordinateur afin de rechercher tout code malveillant éventuel. Dans la fenêtre principale du programme, cliquez sur **Analyse de l'ordinateur**, puis sur **Analyse intelligente**. Pour plus d'informations sur l'analyse de l'ordinateur à la demande, reportez-vous à la section Analyse de l'ordinateur à la demande 9.

2.2 Installation personnalisée

Le mode d'installation personnalisée est destiné aux utilisateurs expérimentés qui souhaitent modifier les paramètres avancés pendant l'installation.

Serveur proxy
Si vous utilisez un serveur proxy, vous pouvez définir ses paramètres maintenant en sélectionnant l'option **J'utilise un serveur proxy**. Entrez ensuite l'adresse IP ou l'adresse URL de votre serveur proxy dans le champ **Adresse**. Dans le champ **Port**, spécifiez le port sur lequel le serveur proxy accepte les connexions (3128 par défaut). Si le serveur proxy exige une authentification, saisissez un **nom d'utilisateur** et un **mot de passe** pour accorder l'accès au serveur proxy. Si vous êtes certain qu'aucun serveur proxy n'est utilisé, choisissez l'option **Je n'utilise pas de serveur proxy**. Si vous n'en êtes pas certain, vous pouvez utiliser vos paramètres système en cours en sélectionnant l'option **Utiliser les paramètres système (recommandée)**.

Privilèges
Dans l'étape suivante, vous pouvez définir les utilisateurs privilégiés qui pourront modifier la configuration du programme. Dans la liste des utilisateurs figurant à gauche, sélectionnez les utilisateurs et l'option **Ajouter** pour les ajouter à la liste **Utilisateurs privilégiés**. Pour afficher tous les utilisateurs du système, sélectionnez l'option **Afficher tous les utilisateurs**. Si la liste Utilisateurs privilégiés est vide, tous les utilisateurs sont considérés comme étant privilégiés.

Live Grid
Le système d'alerte anticipé Live Grid veille à ce qu'ESET soit immédiatement et continuellement informé des nouvelles infiltrations afin de protéger rapidement nos clients. Ce système permet de soumettre de nouvelles menaces au laboratoire d'ESET, où elles sont analysées, traitées et ajoutées à la base des signatures de virus. Par défaut, l'option **Activer le système d'alerte anticipé Live Grid** est sélectionnée. Cliquez sur **Configuration...** pour modifier les paramètres détaillés de soumission des fichiers suspects. Pour plus d'informations, reportez-vous à la section Live Grid 21.

Applications spéciales
L'étape suivante de l'installation consiste à configurer la détection des **applications potentiellement indésirables**. De tels programmes ne sont pas nécessairement malveillants, mais peuvent avoir une incidence négative sur le comportement du système d'exploitation. Ces applications sont souvent associées à d'autres programmes et peuvent être difficiles à remarquer lors de l'installation. Ces applications affichent habituellement une notification pendant l'installation, mais elles peuvent facilement s'installer sans votre consentement.

Pare-feu personnel : mode de filtrage
Lors de la dernière étape, il est possible de sélectionner un mode de filtrage pour le pare-feu personnel. Pour plus d'informations, voir Modes de filtrage 13.

Après l'installation de ESET Cyber Security Pro, vous devez effectuer une analyse de l'ordinateur afin de rechercher tout code malveillant éventuel. Dans la fenêtre principale du programme, cliquez sur **Analyse de l'ordinateur**, puis sur **Analyse intelligente**. Pour plus d'informations sur l'analyse de l'ordinateur à la demande, reportez-vous à la section Analyse de l'ordinateur à la demande 9.

3. Activation du produit

Après l'installation, la fenêtre **Type d'activation de produit** s'affiche automatiquement à l'écran. Vous pouvez aussi cliquer sur l'icône ESET Cyber Security Pro dans la barre de menus (en haut de l'écran), puis sur **Activation du produit...**.

1. Si vous avez acheté une version boîte du produit, sélectionnez l'option **Activation à l'aide d'une clé d'activation**. La clé d'activation se trouve généralement à l'intérieur du coffret ou au dos de celui-ci. Pour permettre l'activation, la clé doit être introduite telle quelle.

2. Si vous recevez un nom d'utilisateur et un mot de passe, sélectionnez l'option **Utiliser un nom d'utilisateur et un mot de passe** et entrez les données de licence dans les champs appropriés. Cette option équivaut à l'option **Configuration du nom d'utilisateur et du mot de passe...** dans la fenêtre **Mettre à jour** du programme.

3. Si vous souhaitez évaluer ESET Cyber Security Pro avant de l'acheter, sélectionnez l'option **Activer la licence d'essai**. Indiquez votre adresse électronique pour activer ESET Cyber Security Pro pendant un laps de temps limité. La licence d'essai vous sera envoyée par courrier électronique. La licence d'essai ne peut être activée qu'une seule fois par client.

Si vous choisissez de ne pas effectuer l'activation maintenant, cliquez sur **Activer ultérieurement**. Vous pouvez directement activer ESET Cyber Security Pro à partir de la section **Accueil** ou **Mise à jour** de la fenêtre du programme principal d'ESET Cyber Security Pro.

Si vous n'avez pas de licence et souhaitez en acheter une, cliquez sur l'option **Licence**. Cette opération vous redirigera vers le site Web de votre distributeur ESET local.

4. Désinstallation

Pour désinstaller ESET Cyber Security Pro de votre ordinateur, effectuez l'une des opérations suivantes :

- insérez le CD/DVD d'installation ESET Cyber Security Pro dans votre ordinateur, ouvrez-le à partir du Bureau ou de la fenêtre **Finder**, puis double-cliquez sur l'icône **Désinstaller**,
- ouvrez le fichier d'installation de ESET Cyber Security Pro (*.dmg*) et double-cliquez sur l'icône **Désinstaller**,
- lancez le **Finder**, ouvrez le dossier **Applications** sur le disque dur, appuyez sur la touche CTRL et cliquez sur l'icône **ESET Cyber Security Pro**, puis sélectionnez l'option d'**affichage du contenu du paquet**. Ouvrez le dossier **Resources** et double-cliquez sur l'icône de **désinstallation**.

5. Brève présentation

La fenêtre principale de ESET Cyber Security Pro est divisée en deux sections principales. La fenêtre principale de droite affiche les informations correspondant à l'option sélectionnée dans le menu principal à gauche.

Voici la description des options disponibles dans le menu principal :

- **Accueil** : fournit des informations sur l'état de protection de votre ordinateur, du pare-feu, d'Internet et de la messagerie, ainsi que sur le contrôle parental.
- **Analyse de l'ordinateur** : cette option permet de configurer et de lancer l'analyse de l'ordinateur à la demande 9.
- **Mettre à jour** : affiche des informations sur les mises à jour de la base de signatures de virus.
- **Configuration** : sélectionnez cette option pour ajuster le niveau de sécurité de votre ordinateur.
- **Outils** : permet d'accéder aux fichiers journaux 17, au planificateur 18, à la quarantaine 19, aux processus en cours 20 et à d'autres fonctions du programme.
- **Aide** : permet d'accéder aux fichiers d'aide, à la base de connaissances sur Internet, au formulaire de demande d'assistance et à d'autres informations sur le programme.

5.1 Raccourcis clavier

Raccourcis clavier disponibles avec ESET Cyber Security Pro :

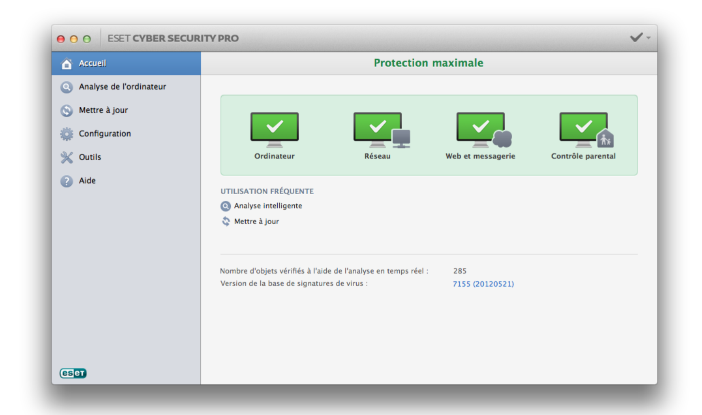
- *cmd-,* : affiche les préférences d'ESET Cyber Security Pro,
- *cmd-U* : ouvre la fenêtre **Configuration du nom d'utilisateur et du mot de passe**,
- *cmd-alt-T* : ouvre la fenêtre **Caractères spéciaux**,
- *cmd-O* : redimensionne la fenêtre de l'interface utilisateur graphique principale d'ESET Cyber Security Pro pour lui redonner sa taille par défaut et la place au centre de l'écran.
- *cmd-alt-H* : masque toutes les fenêtres ouvertes à l'exception d'ESET Cyber Security Pro,
- *cmd-H* - masque ESET Cyber Security Pro.

Les raccourcis claviers suivants ne fonctionnent que si l'option **Utiliser le menu standard** est activée dans **Configuration** > **Saisie des préférences de l'application...** (ou appuyez sur *cmd-,* > **Interface** :

- *cmd-alt-L* : ouvre la section **Fichiers journaux**,
- *cmd-alt-S* : ouvre la section **Planificateur**,
- *cmd-alt-Q* : ouvre la section **Quarantaine**.

5.2 Contrôle du fonctionnement du programme

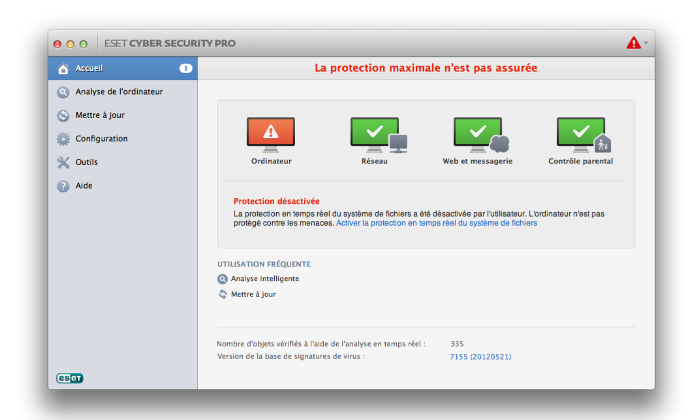
Pour afficher l'état de la protection, cliquez sur l'option **Accueil** dans le menu principal. La fenêtre principale affiche un résumé de l'état de fonctionnement des modules de ESET Cyber Security Pro.



5.3 Que faire lorsque le programme ne fonctionne pas correctement ?

Une icône verte s'affiche en regard de chaque module activé et fonctionnant correctement. Dans le cas contraire, un point d'exclamation rouge ou orange s'affiche. Des informations supplémentaires sur le module et une suggestion de solution du problème sont alors présentées. Pour changer l'état des différents modules, cliquez sur le lien bleu affiché sous chaque message de notification.

Si vous ne parvenez pas à résoudre le problème à l'aide des solutions suggérées, vous pouvez chercher une autre solution dans la base de connaissances ESET ou contacter le Service client ESET. Ce dernier répondra rapidement à vos questions et vous aidera à trouver une solution.



6. Protection de l'ordinateur

La configuration de l'ordinateur se trouve sous **Configuration** > **Ordinateur**. Elle affiche l'état de la **protection en temps réel du système de fichiers** et du **blocage des supports amovibles**. Pour désactiver des modules individuels, réglez le bouton du module en question sur **DÉSACTIVÉ**. Notez que cela peut réduire la protection de votre ordinateur. Pour accéder aux paramètres détaillés de chaque module, cliquez sur le bouton **Configuration...**.

6.1 Protection antivirus et antispyware

La protection antivirus protège des attaques contre le système en modifiant les fichiers représentant des menaces potentielles. Si une menace comportant du code malveillant est détectée, le module Antivirus peut l'éliminer en la bloquant. Il peut ensuite la nettoyer, la supprimer ou la placer en quarantaine.

6.1.1 Protection en temps réel du système de fichiers

La protection en temps réel du système de fichiers vérifie tous les types de supports et déclenche une analyse en fonction de différents événements. Utilisant des méthodes de détection selon la technologie ThreatSense (décrites dans la section intitulée Configuration des paramètres du moteur ThreatSense 10), la protection en temps réel du système de fichiers peut être différente pour les nouveaux fichiers et les fichiers existants. Pour les nouveaux fichiers, il est possible d'appliquer un niveau de contrôle plus approfondi.

Par défaut, la protection en temps réel est lancée au démarrage du système d'exploitation, assurant ainsi une analyse sans interruption. Dans certains cas (par exemple, en cas de conflit avec un autre analyseur en temps réel), il est possible de mettre fin à la protection en temps réel en cliquant sur l'icône ESET Cyber Security Pro dans la barre de menus (en haut de l'écran), puis en sélectionnant l'option **Désactiver la protection en temps réel du système de fichiers** . Il est également possible de mettre fin à la protection en temps réel depuis la fenêtre principale du programme (sélectionnez **Configuration** > **Ordinateur** et réglez **Protection en temps réel du système de fichiers** sur **DÉSACTIVÉ**).

Pour modifier les paramètres avancés de la protection en temps réel, sélectionnez **Configuration** > **Saisie des préférences de l'application...** (ou appuyez sur *cmd-,*) > **Protection en temps réel** et cliquez sur le bouton **Configuration...** situé en regard de l'option **Options avancées** (reportez-vous à la section Options d'analyse avancées 8).

6.1.1.1 Moment de l'analyse (analyse déclenchée par un événement)

Par défaut, tous les fichiers sont analysés à l'ouverture, à la création ou à l'exécution. Il est recommandé de conserver les paramètres par défaut, car ils offrent le niveau maximal de protection en temps réel pour votre ordinateur.

6.1.1.2 Options avancées

Vous pouvez définir dans cette fenêtre les types d'objet que le moteur ThreatSense doit analyser, activer/désactiver l'option **Heuristique avancée** et modifier les paramètres des archives et du cache de fichiers.

Il n'est pas recommandé de modifier les valeurs par défaut de la section **Paramètres d'archive par défaut**, à moins que vous n'ayez besoin de résoudre un problème spécifique, car l'augmentation des valeurs d'imbrication des archives peut avoir une incidence sur les performances.

Vous pouvez activer ou désactiver l'analyse heuristique avancée ThreatSense de chacun des fichiers exécutés, créés et modifiés en sélectionnant ou en désélectionnant la case **Heuristique avancée** de chaque section de paramètres ThreatSense.

Pour réduire l'empreinte système de la protection en temps réel sur le système, vous pouvez définir la taille du cache d'optimisation. Cette fonction est active lorsque vous utilisez l'option **Activer le cache des fichiers nettoyés**. Si cette fonction est désactivée, tous les fichiers sont analysés à chaque accès. Les fichiers ne sont analysés qu'une seule fois après leur mise en cache (sauf s'ils ont été modifiés), jusqu'à ce que la taille définie pour le cache soit atteinte. Les fichiers sont immédiatement réanalysés après chaque mise à jour de la base de signatures de virus. Cliquez sur **Activer le cache des fichiers nettoyés** pour activer/désactiver cette fonction. Pour définir la quantité de fichiers à mettre en cache, il vous suffit d'entrer la valeur souhaitée dans le champ de saisie situé en regard de l'option **Taille du cache**.

D'autres paramètres d'analyse peuvent être définis dans la fenêtre **Configuration du moteur ThreatSense**. Vous pouvez définir, pour la protection en temps réel du système de fichiers, le type des **objets** à analyser, les **options** à utiliser et le niveau de **nettoyage**, les **extensions** et les **limites** de taille de fichiers. Vous pouvez ouvrir la fenêtre de configuration du moteur ThreatSense en cliquant sur le bouton **Configuration...** situé en regard de l'option **Moteur ThreatSense** dans la fenêtre Configuration avancée. Pour plus d'informations sur les paramètres du moteur ThreatSense, reportez-vous à la section Configuration des paramètres du moteur 10.

6.1.1.3 Quand faut-il modifier la configuration de la protection en temps réel ?

La protection en temps réel est le composant essentiel de la sécurisation du système. Procédez avec prudence lorsque vous modifiez les paramètres de protection en temps réel. Il est recommandé de ne modifier ces paramètres que dans des cas très précis. Vous pouvez les modifier par exemple en cas de conflit avec une autre application ou avec l'analyseur en temps réel d'un autre logiciel antivirus.

Après l'installation de ESET Cyber Security Pro, tous les paramètres sont optimisés pour garantir le niveau maximum de système de sécurité aux utilisateurs. Afin de restaurer les paramètres par défaut, cliquez sur le bouton **Par défaut** situé dans la partie inférieure gauche de la fenêtre **Protection en temps réel** (**Configuration** > **Saisie des préférences de l'application...** > **Protection en temps réel**).

6.1.1.4 Vérification de la protection en temps réel

Pour vérifier que la protection en temps réel fonctionne correctement et qu'elle détecte les virus, utilisez le fichier de test eicar.com. Ce fichier de test est un fichier inoffensif particulier qui est détectable par tous les programmes antivirus. Le fichier a été créé par l'institut EICAR (European Institute for Computer Antivirus Research) pour tester la fonctionnalité des programmes antivirus.

6.1.1.5 Que faire si la protection en temps réel ne fonctionne pas ?

Dans ce chapitre, nous décrivons des problèmes qui peuvent survenir lors de l'utilisation de la protection en temps réel et la façon de les résoudre.

La protection en temps réel est désactivée
Si la protection en temps réel a été désactivée par inadvertance par un utilisateur, elle doit être réactivée. Pour réactiver la protection en temps réel, sélectionnez **Configuration** > **Ordinateur** et réglez l'option **Protection en temps réel du système de fichiers** sur **ACTIVÉ**. Vous pouvez également activer la protection en temps réel du système de fichiers dans la fenêtre des préférences de l'application : sous **Protection en temps réel**, sélectionnez **Activer la protection en temps réel du système de fichiers**.



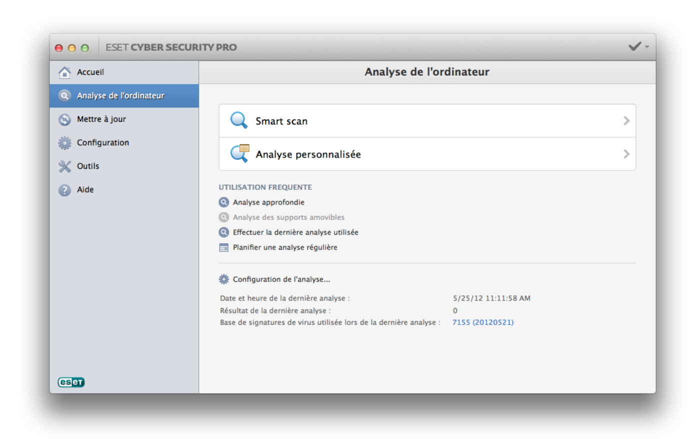
La protection en temps réel ne détecte et ne nettoie pas les infiltrations
Assurez-vous qu'aucun autre programme antivirus n'est installé sur votre ordinateur. Si deux programmes de protection en temps réel sont activés en même temps, il peut y avoir un conflit entre les deux. Il est recommandé de désinstaller tout autre antivirus de votre système.

La protection en temps réel ne démarre pas
Si la protection en temps réel n'est pas initialisée au démarrage du système, cela peut provenir de conflits avec d'autres programmes. Dans ce cas, consultez les spécialistes du service client ESET.

6.1.2 Analyse de l'ordinateur à la demande

Si vous pensez que votre ordinateur peut être infecté (en raison d'un comportement anormal), exécutez **Analyse de l'ordinateur** > **Analyse intelligente** pour rechercher d'éventuelles infiltrations. Pour une protection maximale, les analyses d'ordinateur doivent être exécutées régulièrement dans le cadre de mesures de sécurité de routine. Elles ne doivent pas être exécutées uniquement lorsqu'une infection est suspectée. Une analyse régulière peut détecter des infiltrations non détectées par l'analyseur en temps réel au moment de leur enregistrement sur le disque. Cela peut se produire si l'analyseur en temps réel est désactivé au moment de l'infection ou si la base de signatures de virus n'est plus à jour.

Nous recommandons d'exécuter une analyse de l'ordinateur à la demande au moins une fois par mois. L'analyse peut être configurée comme tâche planifiée dans **Outils** > **Planificateur**.



Vous pouvez également faire glisser les fichiers et dossiers sélectionnés sur votre Bureau ou dans la fenêtre du **Finder** et les faire glisser dans l'écran principal de ESET Cyber Security Pro, sur l'icône du Dock, de la barre de menus (en haut de l'écran) ou de l'application (dans le dossier */Applications*).

6.1.2.1 Type d'analyse

Deux types d'analyses de l'ordinateur à la demande sont disponibles. L'**analyse intelligente** analyse le système sans exiger de configuration plus précise des paramètres d'analyse. L'**analyse personnalisée** permet de sélectionner l'un des profils d'analyse prédéfinis, ainsi que de choisir des cibles spécifiques à analyser.

6.1.2.1.1 Analyse intelligente

L'analyse intelligente permet de lancer rapidement une analyse de l'ordinateur et de nettoyer les fichiers infectés sans intervention de l'utilisateur. Elle présente l'avantage d'être facile à utiliser, sans aucune configuration d'analyse détaillée. L'analyse intelligente vérifie tous les fichiers de tous les dossiers, et nettoie ou supprime automatiquement les infiltrations détectées. Le niveau de nettoyage est automatiquement réglé sur sa valeur par défaut. Pour plus d'informations sur les types de nettoyage, reportez-vous à la section Nettoyage 11.

6.1.2.1.2 Analyse personnalisée

L'**analyse personnalisée** est la solution optimale si vous souhaitez spécifier des paramètres d'analyse tels que les cibles et les méthodes d'analyse. Elle permet en effet de configurer les paramètres avec grande précision. Les configurations peuvent être enregistrées sous forme de profils d'analyse définis par l'utilisateur. Elles permettent d'effectuer régulièrement la même analyse avec les mêmes paramètres.

Pour sélectionner des cibles à analyser, sélectionnez **Analyse de l'ordinateur** > **Analyse personnalisée**, puis les **cibles à analyser** dans la structure arborescente. Une cible à analyser peut également être spécifiée plus précisément : vous devez indiquer le chemin d'accès au dossier ou aux fichiers à inclure. Si vous souhaitez uniquement effectuer une analyse du système sans ajouter d'actions de nettoyage supplémentaires, sélectionnez l'option **Analyse sans nettoyage**. Vous pouvez également choisir parmi trois niveaux de nettoyage en cliquant sur **Configuration...** > **Nettoyage**.

REMARQUE : L'exécution d'analyses personnalisées est recommandée pour les utilisateurs chevronnés qui maîtrisent l'utilisation de programmes antivirus.

6.1.2.2 Cibles à analyser

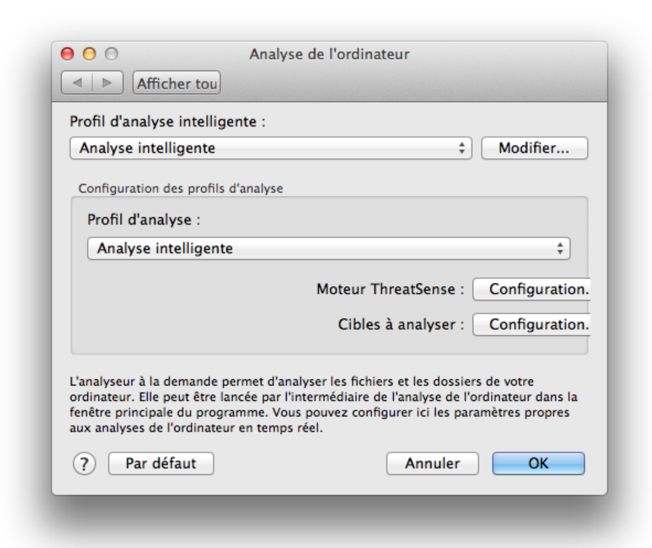
La structure arborescente des cibles à analyser permet de sélectionner les fichiers et dossiers à soumettre à l'analyse antivirus. Les dossiers peuvent également être sélectionnés en fonction des paramètres du profil.

Une cible à analyser peut aussi être définie plus précisément en entrant le chemin du dossier ou des fichiers à inclure dans l'analyse. Sélectionnez les cibles dans la structure arborescente des dossiers disponibles sur l'ordinateur.

6.1.2.3 Profils d'analyse

Vos paramètres d'analyse préférés peuvent être enregistrés pour les prochaines analyses. Il est recommandé de créer autant de profils (avec différentes cibles et méthodes, et d'autres paramètres d'analyse) que d'analyses utilisées régulièrement.

Pour créer un profil, sélectionnez **Configuration** > **Saisie des préférences de l'application...** (ou appuyez sur *cmd-,*) > **Analyse de l'ordinateur** et cliquez sur l'option **Modifier...** en regarde de la liste des profils en cours.



Pour plus d'informations sur la création d'un profil d'analyse, reportez-vous à la section Configuration des paramètres du moteur ThreatSense 10 ; vous y trouverez une description de chaque paramètre de configuration de l'analyse.

Exemple : Supposons la situation suivante : vous souhaitez créer votre propre profil d'analyse, la configuration d'analyse intelligente est partiellement adéquate, mais vous ne souhaitez analyser ni les fichiers exécutables compressés, ni les applications potentiellement dangereuses. Vous souhaitez effectuer un nettoyage strict. Dans la fenêtre **Liste des profils de l'analyseur à la demande**, saisissez le nom du profil, cliquez sur le bouton **Ajouter** et confirmez en cliquant sur **OK**. Réglez ensuite les paramètres pour qu'ils correspondent à vos besoins en configurant les options **Moteur ThreatSense** et **Cibles à analyser**.

6.1.3 Exclusions

Cette section (**Configuration** > **Saisie des préférences de l'application...** > **Exclusions**) permet d'exclure de l'analyse certains fichiers/dossiers, applications ou adresses IP/IPv6.

Les fichiers et les dossiers répertoriés dans la liste **Système de fichiers** seront exclus de tous les analyseurs : système (au démarrage), en temps réel et à la demande.

- **Chemin** : chemin d'accès aux fichiers et dossiers exclus.
- **Menace** : si le nom d'une menace figure en regard d'un fichier exclu, cela signifie que ce fichier n'est exclu que pour cette menace spécifique : il n'est pas exclu complètement. Par conséquent, si le fichier est infecté ultérieurement par un autre logiciel malveillant, il est détecté par le module antivirus.
- **Ajouter...** : exclut les objets de la détection. Saisissez le chemin d'accès à l'objet (vous pouvez également utiliser les caractères génériques *** et *?*) ou sélectionnez le dossier ou le fichier dans la structure arborescente.
- **Modifier...** : permet de modifier des entrées sélectionnées.
- **Supprimer** : supprime les entrées sélectionnées.
- **Par défaut** : annule toutes les exclusions.

Dans l'onglet **Internet et messagerie**, il est possible d'exclure certaines **Applications** ou **adresses IP/IPv6** de l'analyse des protocoles.

6.1.4 Configuration des paramètres du moteur ThreatSense

ThreatSense est la technologie propriétaire d'ESET consistant en une combinaison de méthodes complexes de détection de menaces. Cette technologie est proactive : elle fournit une protection dès les premières heures de propagation d'une nouvelle menace. Elle utilise une combinaison de plusieurs méthodes (analyse de code, émulation de code, signatures génériques, signatures de virus) qui se conjuguent pour améliorer sensiblement la sécurité du système. Ce moteur d'analyse est capable de contrôler plusieurs flux de données simultanément, optimisant ainsi l'efficacité et le taux de détection. La technologie ThreatSense protège également des rootkits.

Les options de configuration de la technologie ThreatSense permettent de spécifier plusieurs paramètres d'analyse :

- les types de fichiers et les extensions à analyser ;
- la combinaison de plusieurs méthodes de détection ;
- les niveaux de nettoyage, etc.

Pour définir les utilisateurs privilégiés, sélectionnez **Configuration > Saisie des préférences de l'application...** (ou appuyez sur *cmd-,*), puis cliquez sur le bouton **Configuration du moteur ThreatSense...** situé dans les zones **Protection du système**, **Protection en temps réel** et **Analyse de l'ordinateur**, qui utilisent toutes la technologie ThreatSense (voir ci-dessous). Chaque scénario de sécurité peut exiger une configuration différente. ThreatSense est configurable individuellement pour les modules de protection suivants :

- **Protection du système** : vérification automatique des fichiers de démarrage
- **Protection en temps réel** : protection en temps réel du système de fichiers
- **Analyse de l'ordinateur** : analyse de l'ordinateur à la demande

Les paramètres ThreatSense sont optimisés pour chaque module et leur modification peut avoir une incidence significative sur le fonctionnement du système. Par exemple, en modifiant les paramètres pour toujours analyser les fichiers exécutables compressés ou pour activer l'analyse heuristique avancée dans le module de protection en temps réel du système de fichiers, vous pouvez dégrader les performances du système. Il est donc recommandé de ne pas modifier les paramètres ThreatSense par défaut pour tous les modules, à l'exception du module Analyse de l'ordinateur.

6.1.4.1 Objets

La section **Objets** permet de définir les fichiers de l'ordinateur qui vont faire l'objet d'une analyse visant à rechercher les éventuelles infiltrations.

- **Fichiers** : analyse tous les types de fichiers courants (programmes, images, musiques, vidéos, bases de données, etc.).
- **Liens symboliques** : (analyseur à la demande uniquement) analyse un type spécial de fichiers qui contiennent une chaîne de texte interprétée par le système d'exploitation comme chemin d'accès à un autre fichier ou répertoire.
- **Envoyer les fichiers par courrier électronique** : (non disponible dans la protection en temps réel) analyse des fichiers contenant des messages électroniques.
- **Boîtes aux lettres** : (non disponible dans la protection en temps réel) analyse les boîtes aux lettres de l'utilisateur stockées dans le système. L'utilisation inadéquate de cette option peut provoquer des conflits avec votre client de messagerie. Pour en savoir plus sur les avantages et les inconvénients de cette option, reportez-vous à cet article de base de connaissances.
- **Archives** : (non disponible dans la protection en temps réel) analyse les fichiers compressés dans les archives (.rar, .zip, .arj, .tar, etc.).
- **Archives auto-extractibles** : (non disponible dans la protection en temps réel) analyse les fichiers contenus dans des fichiers d'archives auto-extractibles.
- **Fichiers exécutables compressés** : contrairement aux types d'archives standard, les fichiers exécutables compressés sont décompressés en mémoire, en plus des fichiers exécutables compressés statiques standard (UPX, yoda, ASPack, FGS, etc.).

6.1.4.2 Options

Vous pouvez sélectionner dans la section **Options** les méthodes utilisées lors de la recherche d'infiltrations dans le système. Les options disponibles sont les suivantes :

- **Heuristique** : l'heuristique est un algorithme qui analyse l'activité (malveillante) des programmes. La détection heuristique présente l'avantage de détecter les nouveaux logiciels malveillants qui n'existaient pas auparavant ou qui ne figurent pas dans la liste des virus connus (base de signatures de virus).
- **Heuristique avancée** : cette option utilise un algorithme heuristique unique développé par ESET et optimisé pour la détection de vers informatiques et de chevaux de Troie écrits dans des langages de programmation de haut niveau. L'heuristique avancée améliore de manière significative la capacité de détection du programme.
- **Applications potentiellement indésirables** : ces applications ne sont pas nécessairement malveillantes, mais elles peuvent avoir une incidence négative sur les performances de votre ordinateur. L'installation de ces applications nécessite généralement l'accord de l'utilisateur. Si elles sont présentes sur votre ordinateur, votre système se comporte différemment (par rapport à son état avant l'installation de ces applications). Les changements les plus significatifs concernent l'affichage indésirable de fenêtres contextuelles, l'activation et l'exécution de processus cachés, l'augmentation de l'utilisation des ressources système, les changements dans les résultats de recherche et les applications communiquant avec des serveurs distants.
- **Applications potentiellement dangereuses** : cette appellation fait référence à des logiciels commerciaux légitimes qui peuvent être mis à profit par des pirates, s'ils ont été installés à l'insu de l'utilisateur. La classification inclut des programmes tels que des outils d'accès à distance. C'est pour cette raison que cette option est désactivée par défaut.

6.1.4.3 Nettoyage

Les paramètres de nettoyage déterminent la façon dont l'analyseur nettoie les fichiers infectés. Trois niveaux de nettoyage sont possibles :

- **Pas de nettoyage** : les fichiers infectés ne sont pas nettoyés automatiquement. Le programme affiche une fenêtre d'alerte et permet à l'utilisateur de choisir une action.
- **Nettoyage standard** : le programme essaie de nettoyer ou de supprimer automatiquement tout fichier infecté. S'il n'est pas possible de sélectionner automatiquement l'action requise, le programme propose une sélection d'actions de suivi. Cette sélection s'affiche également si une action prédéfinie ne peut pas être menée à bien.
- **Nettoyage strict** : le programme nettoie ou supprime tous les fichiers infectés (y compris les archives). Les seules exceptions sont les fichiers système. S'il n'est pas possible de les nettoyer, la fenêtre d'alerte qui s'affiche propose différentes options.

Avertissement : En mode de nettoyage standard par défaut, le fichier d'archive n'est entièrement supprimé que si tous les fichiers qu'il contient sont infectés. Si l'archive contient également des fichiers légitimes, elle n'est pas supprimée. Si un fichier d'archive infecté est détecté en mode Nettoyage strict, le fichier entier est supprimé, même s'il contient également des fichiers intacts.

6.1.4.4 Extensions

L'extension est la partie du nom de fichier située après le point. Elle définit le type et le contenu du fichier. Cette section de la configuration des paramètres ThreatSense vous permet de définir les types de fichiers à exclure de l'analyse.

Par défaut, tous les fichiers sont analysés, quelle que soit leur extension. Toutes les extensions peuvent être ajoutées à la liste des fichiers exclus de l'analyse. Les boutons **Ajouter** et **Supprimer** permettent d'activer ou d'empêcher l'analyse des extensions souhaitées.

L'exclusion de certains fichiers de l'analyse peut être utile si l'analyse de ces fichiers provoque un dysfonctionnement du programme. Par exemple, il peut être judicieux d'exclure les extensions *.log*, *.cfg* et *.tmp*.

6.1.4.5 Limites

La section **Limites** permet de spécifier la taille maximale des objets et les niveaux d'imbrication des archives à analyser :

- **Taille maximale :** définit la taille maximum des objets à analyser. Le module antivirus n'analyse alors que les objets d'une taille inférieure à celle spécifiée. Il n'est pas recommandé de modifier la valeur par défaut et il n'y a généralement aucune raison de le faire. Cette option ne doit être modifiée que par des utilisateurs chevronnés ayant des raisons très précises d'exclure de l'analyse les objets plus volumineux.
- **Durée maximale d'analyse :** définit la durée maximum attribuée à l'analyse d'un objet. Si la valeur de ce champ a été définie par l'utilisateur, le module antivirus cesse d'analyser un objet une fois ce temps écoulé, que l'analyse soit terminée ou non.
- **Niveau d'imbrication maximal :** indique la profondeur maximale d'analyse des archives. Il n'est pas recommandé de modifier la valeur par défaut (10). Dans des circonstances normales, il n'y a aucune raison de le faire. Si l'analyse prend fin prématurément en raison du nombre d'archives imbriquées, l'archive reste non vérifiée.
- **Taille de fichiers maximale :** cette option permet de spécifier la taille maximale (après extraction) des fichiers à analyser qui sont contenus dans les archives. Si l'analyse prend fin prématurément en raison de cette limite, l'archive reste non vérifiée.

6.1.4.6 Autres

Activer l'optimisation intelligente
Lorsque l'option Optimisation intelligente est activée, les paramètres sont optimisés de manière à garantir le niveau d'analyse le plus efficace sans compromettre la vitesse d'analyse. Les différents modules de protection proposent une analyse intelligente en utilisant différentes méthodes. L'option Optimisation intelligente n'est pas définie de manière fixe dans le produit. L'équipe de développement d'ESET met en œuvre en permanence de nouvelles modifications qui sont ensuite intégrées dans ESET Cyber Security Pro par l'intermédiaire de mises à jour régulières. Si l'option Optimisation intelligente est désactivée, seuls les paramètres définis par l'utilisateur dans le noyau ThreatSense de ce module particulier sont appliqués lors de la réalisation d'une analyse.

Analyser l'autre flux de données (analyseur à la demande uniquement)
Les autres flux de données (branchements de ressources/données) utilisés par le système de fichiers sont des associations de fichiers et de dossiers invisibles pour les techniques ordinaires d'analyse. De nombreuses infiltrations tentent d'éviter la détection en se faisant passer pour d'autres flux de données.

6.1.5 Une infiltration est détectée

Des infiltrations peuvent atteindre le système à partir de différents points d'entrée : pages Web, dossiers partagés, courrier électronique ou périphériques amovibles (USB, disques externes, CD, DVD, etc.).

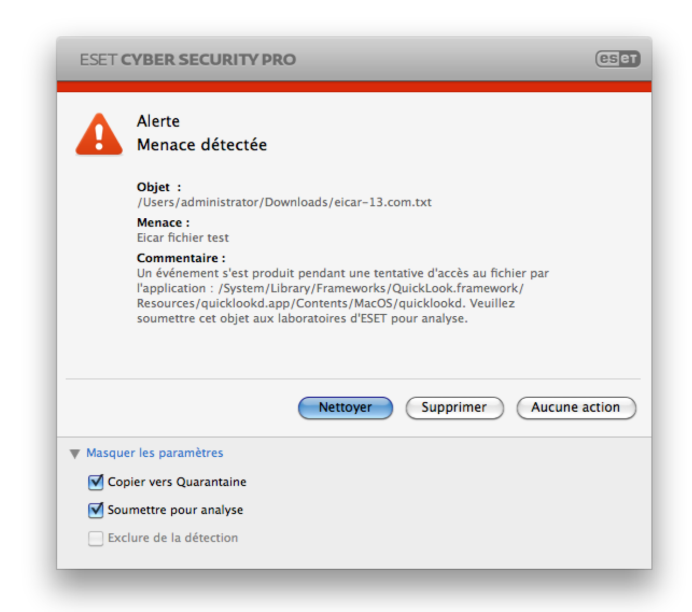
Si votre ordinateur montre des signes d'infection par un logiciel malveillant (ralentissement, blocages fréquents, etc.), nous recommandons d'effectuer les opérations suivantes :

1. Cliquez sur **Analyse de l'ordinateur**.
2. Cliquez sur **Analyse intelligente** (pour plus d'informations, reportez-vous à la section Analyse intelligente 9).
3. Lorsque l'analyse est terminée, consultez le journal pour connaître le nombre de fichiers analysés, infectés et nettoyés.

Si vous ne souhaitez analyser qu'une certaine partie de votre disque, cliquez sur **Analyse personnalisée** et sélectionnez les cibles à analyser.

Pour donner un exemple général du traitement des infiltrations dans ESET Cyber Security Pro, supposons qu'une infiltration soit détectée par la protection en temps réel du système de fichiers, qui utilise le niveau de nettoyage par défaut. Le programme tente de nettoyer ou de supprimer le fichier. Si aucune action n'est prédéfinie pour le module de protection en temps réel, vous êtes invité à sélectionner une option dans une fenêtre d'alerte. Généralement, les options **Nettoyer**, **Supprimer** et **Aucune action** sont disponibles. Il n'est pas recommandé de sélectionner **Aucune action**, car les fichiers infectés seraient conservés tels quels. La seule exception concerne les situations où vous êtes sûr que le fichier est inoffensif et a été détecté par erreur.

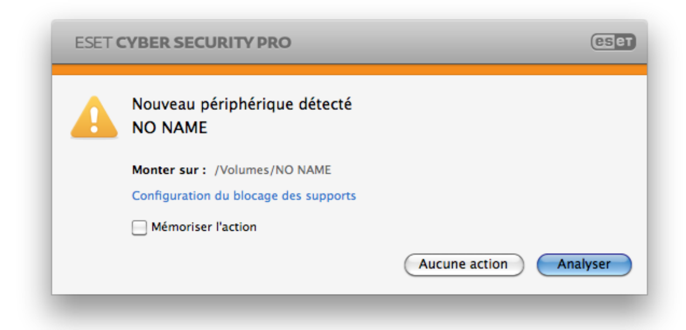
Nettoyage et suppression : utilisez le nettoyage si un fichier a été attaqué par un virus qui y a joint du code malveillant. Dans ce cas, essayez d'abord de nettoyer le fichier infecté pour le restaurer dans son état d'origine. Si le fichier se compose uniquement de code malveillant, il sera supprimé.



Suppression de fichiers dans des archives : en mode de nettoyage par défaut, l'archive complète n'est supprimée que si elle ne contient que des fichiers infectés et aucun fichier sain. Autrement dit, les archives ne sont pas supprimées si elles contiennent également des fichiers sains. Cependant, soyez prudent si vous choisissez un **nettoyage strict** : dans ce mode, l'archive est supprimée si elle contient au moins un fichier infecté, quel que soit l'état des autres fichiers qu'elle contient.

6.2 Analyse et blocage de supports amovibles

ESET Cyber Security Pro offre une analyse à la demande du support amovible introduit (CD, DVD, USB, périphérique iOS, etc.).



Les supports amovibles peuvent contenir du code malveillant et constituer un risque pour votre ordinateur. Pour bloquer des supports amovibles, cliquez sur **Configuration du blocage des supports** (voir l'illustration ci-dessus) ou sur **Configuration** > **Saisie des préférences de l'application...** > **Supports** dans la fenêtre principale du programme et activez l'option **Activer le blocage des supports amovibles**. Pour autoriser l'accès à certains types de supports, désélectionnez les volumes souhaités.

REMARQUE : Pour autoriser l'accès à un lecteur de CD-ROM externe connecté à votre ordinateur par le biais d'un câble USB, désactivez l'option **CD-ROM**.

7. Pare-feu

Le pare-feu personnel contrôle tout le trafic réseau entrant et sortant sur le système. Pour ce faire, il autorise ou refuse les connexions réseau individuelles en fonction de règles de filtrage spécifiées. Il offre une protection contre les attaques provenant d'ordinateurs distants et permet de bloquer certains services. Il assure aussi une protection antivirus pour les protocoles HTTP, POP3 et IMAP. Cette fonctionnalité constitue un élément très important de la sécurité informatique.

La configuration du pare-feu personnel se trouve sous **Configuration** > **Pare-feu**. Elle permet d'ajuster le mode de filtrage, les règles et les paramètres détaillés. Elle permet aussi d'accéder à des paramètres plus détaillés du programme.

Si vous réglez **Bloquer tout le trafic réseau : déconnecter le réseau** sur **ACTIVÉ**, le pare-feu personnel bloquera toutes les communications entrantes et sortantes. Utilisez cette option uniquement si vous suspectez des risques critiques pour la sécurité exigeant de déconnecter le système du réseau.

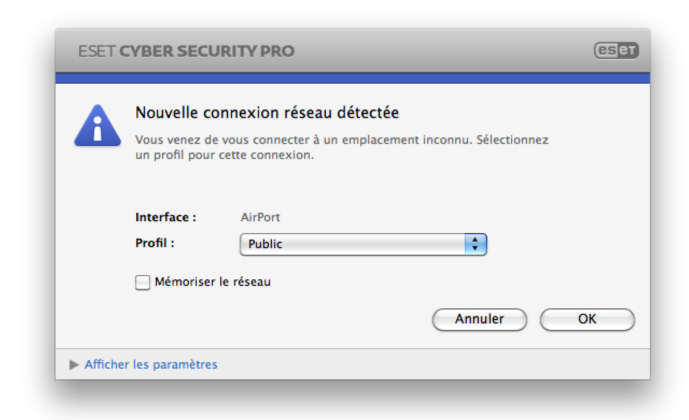
7.1 Modes de filtrage

Trois modes de filtrage sont disponibles pour le pare-feu personnel de ESET Cyber Security Pro. Ces modes se trouvent dans les préférences ESET Cyber Security Pro (appuyez sur *cmd-,*) > **Pare-feu**. Le comportement du pare-feu change en fonction du mode sélectionné. Les modes de filtrage influencent aussi le niveau d'intervention requis de la part de l'utilisateur.

Tout le trafic est bloqué : toutes les connexions entrantes et sortantes sont bloquées.

Automatique avec exceptions : c'est le mode par défaut. Il convient pour les utilisateurs qui préfèrent une utilisation simple et pratique du pare-feu, sans devoir définir de règles. Le mode automatique autorise le trafic sortant standard pour le système concerné et bloque toutes les connexions non lancées provenant du côté réseau. Vous pouvez aussi ajouter des règles personnalisées définies par l'utilisateur.

Mode interactif : permet une configuration personnalisée de votre pare-feu personnel. Lorsqu'une communication est détectée et qu'aucune règle existante ne s'applique à cette communication, une boîte de dialogue s'affiche pour signaler une connexion inconnue. Ce dialogue permet d'autoriser ou de refuser la communication et cette décision peut être mémorisée sous la forme d'une nouvelle règle du pare-feu personnel. Si vous choisissez de créer une règle à ce stade, toutes les connexions futures de ce type seront autorisées ou bloquées selon cette règle.



Si vous souhaitez enregistrer des informations détaillées sur toutes les connexions bloquées dans un fichier journal, sélectionnez l'option **Consigner toutes les connexions bloquées**. Pour consulter les fichiers journaux du pare-feu, cliquez sur **Outils** > **Journaux**, puis sélectionnez **Pare-feu** dans le menu déroulant **Journal**.

7.2 Règles de pare-feu

Les règles sont un ensemble de conditions utilisées pour tester de manière intelligente toutes les connexions réseau et toutes les actions assignées à ces conditions. Le pare-feu personnel permet de définir l'action à entreprendre lorsqu'une connexion définie par une règle est établie.

Les connexions entrantes sont initiées par un ordinateur distant qui tente d'établir une connexion avec le système local. Les connexions sortantes fonctionnent en sens inverse : c'est le système local qui contacte un ordinateur distant.

Si une nouvelle communication inconnue est détectée, vous devez bien réfléchir à savoir si vous voulez l'autoriser ou la refuser. Des connexions non sollicitées, non sécurisées ou inconnues constituent un risque pour la sécurité du système. Si une telle connexion est établie, nous recommandons de prêter une attention particulière à l'ordinateur distant et à l'application qui tentent de se connecter à votre ordinateur. Nombre d'infiltrations tentent d'obtenir et d'envoyer des données privées ou de télécharger d'autres applications malveillantes sur des postes de travail hôtes. Le pare-feu personnel permet de détecter et de mettre fin à ces connexions.

7.2.1 Création d'une règle

L'onglet **Règles** contient une liste de toutes les règles appliquées sur le trafic générés par les différentes applications. Des règles sont ajoutées automatiquement en fonction des réactions de l'utilisateur face à une nouvelle communication.

Pour créer une règle, cliquez sur le bouton**Ajouter...**, entrez le nom de la règle et faites glisser l'icône de l'application sur le champ carré vide ou cliquez sur **Parcourir...** pour chercher le programme dans le dossier */Applications*. Si vous souhaitez appliquer la règle à toutes les applications installées sur votre ordinateur, sélectionnez l'option **Toutes les applications**.

Dans l'étape suivante, spécifiez l'**action** (autoriser ou refuser la communication entre l'application sélectionnée et le réseau) et la **direction** de la communication (entrante, sortante ou les deux). Si vous souhaitez enregistrer toutes les communications liées à cette règle dans un fichier journal, sélectionnez l'option **Règle de consignation**. Pour consulter les journaux, cliquez sur **Outils** > **Journaux** dans le menu principal de ESET Cyber Security Pro, puis sélectionnez **Pare-feu** dans le menu déroulant **Journal**.

Dans la section **Protocole/Ports**, sélectionnez un protocole utilisé pour les communications de l'application et les numéros de port (si le protocole TCP ou UDP est sélectionné). La couche du protocole de transport assure un transfert sûr et efficace des données.

La dernière étape consiste à spécifier la destination (adresse IP, plage, sous-réseau, Ethernet ou Internet).

7.3 Zones de pare-feu

Une zone est un ensemble d'adresses réseau constituant un groupe logique. Chaque adresse d'un groupe donné se voit assigner des règles similaires définies de manière centralisée pour l'ensemble du groupe.

Ces zones peuvent être créées en cliquant sur le bouton **Ajouter...**. Entrez le **nom** et la **description** (facultative) de la zone, choisissez un profil à associer à la zone et ajoutez une adresse IPv4/IPv6, une plage d'adresses, un sous-réseau, un réseau WiFi ou une interface.

7.4 Profils de pare-feu

Les **profils** permettent de contrôler le comportement du pare-feu personnel de ESET Cyber Security Pro. Lorsque vous créez ou modifiez une règle de pare-feu personnel, vous pouvez l'affecter à un profil spécifique ou l'appliquer à tous les profils. Lorsque vous sélectionnez un profil, seules les règles globales (sans profil spécifié) et les règles assignées à ce profil sont appliquées. Vous pouvez créer plusieurs profils avec des règles différentes pour modifier facilement le comportement du pare-feu personnel.

7.5 Journaux de pare-feu

Le pare-feu personnel de ESET Cyber Security Pro enregistre tous les événements importants dans un fichier journal, qui peut être consulté directement à partir du menu principal. Cliquez sur **Outils** > **Journaux**, puis sélectionnez **Pare-feu** dans le menu déroulant **Journal**.

Les fichiers journaux sont un outil précieux pour détecter les erreurs et révéler les intrusions dans votre système. Le pare-feu personnel d'ESET contient les données suivantes :

- Date et heure de l'événement
- Nom de l'événement
- Source
- Adresse réseau cible
- Protocole de communication réseau
- Règle appliquée ou nom du ver éventuellement identifié
- Application impliquée
- Utilisateur

Une analyse approfondie de ces données peut aider à détecter des tentatives visant à compromettre la sécurité du système. De nombreux autres facteurs indiquent des risques potentiels pour la sécurité et vous permettent d'en minimiser l'impact : connexions trop fréquentes à partir d'emplacements inconnus, tentatives multiples d'établir des connexions, communications d'applications inconnues ou utilisation de numéros de ports inhabituels.

8. Protection Internet et messagerie

La configuration de la Protection Internet et messagerie se trouve sous **Configuration** > **Internet et messagerie**. Elle permet aussi d'accéder aux paramètres détaillés de chaque module.

Protection de l'accès Web et antihameçonnage : si elle est activée (ce qui est recommandé), la protection du système de fichiers en temps réel surveille en permanence tous les événements liés à l'antivirus.

Protection du client de messagerie : permet de contrôler la communication par courrier électronique effectuée via les protocoles POP3 et IMAP.

8.1 Protection Web

La protection de l'accès Web surveille la communication entre les navigateurs Web et les serveurs distants et respecte les règles du protocole HTTP (Hypertext Transfer Protocol).

8.1.1 Ports

L'onglet **Ports** permet de définir les numéros de port utilisés pour la communication HTTP. Par défaut, les numéros de port 80, 8080 et 3128 sont prédéfinis.

8.1.2 Mode actif

ESET Cyber Security Pro contient également le sous-menu **Mode actif**, qui définit le mode de contrôle des navigateurs Web. Le mode actif examine les données transférées à partir d'applications accédant à Internet en général, qu'elles soient ou nom qualifiées de navigateurs Web. S'il n'est pas activé, la communication des applications est surveillée progressivement par lots. Cela réduit l'efficacité de la vérification des données, mais assure aussi une plus grande compatibilité des applications. Si aucun problème ne se produit lors de son utilisation, nous recommandons d'activer le mode actif en activant la case en regard de l'application concernée.

Lorsqu'une application contrôlée télécharge des données, celles-ci sont d'abord enregistrées dans un fichier temporaire créé par ESET Cyber Security Pro. À ce stade, les données ne sont pas disponibles pour l'application en question. Une fois que le téléchargement est terminé, les données sont soumises à une recherche de code malveillant. Si aucune infiltration n'est détectée, les données sont envoyées à l'application d'origine. Ce processus assure un contrôle complet des communications d'une application contrôlée. Si le mode passif est activé, les données sont fournies peu à peu à l'application d'origine pour éviter les expirations de délais.

8.1.3 Listes d'URL

La section **Listes d'URL** permet de spécifier des adresses HTTP à bloquer, à autoriser ou à exclure du contrôle. Les sites Web figurant dans la liste des adresses bloquées ne seront pas accessibles. Les sites Web répertoriés dans la liste des adresses exclues sont accessibles sans recherche de code malveillant.

Si vous souhaitez réserver l'accès aux adresses URL figurant dans la liste des **URL autorisées**, sélectionnez l'option **Limiter les adresses URL**.

Pour activer une liste, sélectionnez l'option **Activé**. Si vous souhaitez être averti lors de la saisie d'une adresse figurant dans la liste courante, sélectionnez l'option **Notifiée**.

Dans toutes les listes, vous pouvez utiliser les symboles spéciaux *** (astérisque) et *?* (point d'interrogation). L'astérisque remplace toute chaîne de caractères, tandis que le point d'interrogation remplace n'importe quel caractère. Soyez particulièrement prudent dans la définition des adresses exclues, car la liste ne doit contenir que des adresses fiables et sûres. De même, il faut veiller à utiliser correctement les symboles * et ? dans cette liste.

8.2 Protection de la messagerie

La protection de la messagerie permet de contrôler la communication par courrier électronique effectuée via les protocoles POP3 et IMAP. Lorsqu'il examine les messages entrants, le programme utilise toutes les méthodes d'analyse avancées offertes par le moteur d'analyse ThreatSense. La détection des programmes malveillants s'effectue donc avant même leur comparaison avec la base des signatures de virus. L'analyse des communications suivant les protocoles POP3 et IMAP est indépendante du client de messagerie utilisé.

Moteur ThreatSense : la configuration avancée de l'analyseur de virus permet de configurer les cibles à analyser, les méthodes de détection, etc. Cliquez sur **Configuration...** pour afficher la fenêtre de configuration détaillée de l'analyseur.

Après la vérification d'un message, une notification peut y être ajoutée avec les résultats de l'analyse. Vous pouvez choisir d' **ajouter les notifications à l'objet des messages**. Ne vous fiez pas aveuglément à ces notifications, car elles peuvent ne pas figurer dans des messages HTML problématiques ou être contrefaites par certains virus. Les options disponibles sont les suivantes :

Jamais : aucune notification ne sera ajoutée ;
Courriers infectés uniquement : seuls les messages contenant des logiciels malveillants seront marqués comme vérifiés ;
Tous les courriers analysés : le programme ajoute une notification à chaque message analysé.

Modèle ajouté à l'objet du courrier infecté : modifiez ce modèle si vous souhaitez changer le format du préfixe ajouté à l'objet d'un message infecté.

Ajouter la notification à la note de bas de page du message : activez cette case pour insérer une alerte de virus dans le message infecté. Cette fonctionnalité permet un filtrage simple des messages infectés. Elle augmente aussi le niveau de crédibilité vis-à-vis du destinataire et, en cas de détection d'une infiltration, elle fournit des informations précieuses sur le niveau de menace d'un message ou d'un expéditeur donné.

8.2.1 Vérification par protocole POP3

Le protocole POP3 est le protocole le plus répandu pour la réception de courrier électronique dans un client de messagerie. ESET Cyber Security Pro assure la protection de ce protocole quel que soit le client de messagerie utilisé.

Le module de protection assurant cette vérification est automatiquement lancé au démarrage du système et reste ensuite actif en mémoire. Pour que le module fonctionne correctement, assurez-vous qu'il est activé ; le contrôle du protocole POP3 est effectué automatiquement sans qu'il soit nécessaire de reconfigurer le client de messagerie. Par défaut, toutes les communications sur le port 110 sont analysées, mais vous pouvez y ajouter d'autres ports de communication au besoin. Les numéros de ports doivent être séparés par des virgules.

Si l'option **Activer la vérification par protocole POP3** est activée, tout le trafic passant par POP3 fait l'objet d'un contrôle des logiciels malveillants.

8.2.2 Vérification par protocole IMAP

Le protocole IMAP (Internet Message Access Protocol) est un autre protocole Internet destiné à la récupération de courrier électronique. IMAP présente certains avantages par rapport à POP3. Il permet notamment la connexion simultanée de plusieurs clients à la même boîte aux lettres et permet de conserver les informations d'état des messages telles que le fait de savoir si le message a été lu, si une réponse a été envoyée ou s'il a été supprimé. ESET Cyber Security Pro offre une protection pour ce protocole quel que soit le client de messagerie utilisé.

Le module de protection assurant cette vérification est automatiquement lancé au démarrage du système et reste ensuite actif en mémoire. Pour que le module fonctionne correctement, assurez-vous qu'il est activé ; le contrôle du protocole IMAP est effectué automatiquement sans qu'il soit nécessaire de reconfigurer le client de messagerie. Par défaut, toutes les communications sur le port 143 sont analysées, mais vous pouvez y ajouter d'autres ports de communication au besoin. Les numéros de ports doivent être séparés par des virgules.

Si l'option **Activer la vérification par protocole IMAP** est activée, tout le trafic passant par IMAP fait l'objet d'un contrôle des logiciels malveillants.

9. Contrôle parental

La section **Contrôle parental** permet de configurer les paramètres du contrôle parental, qui offrent aux parents des outils automatisés avec lesquels ils peuvent protéger leurs enfants. L'objectif est d'empêcher les enfants et les adolescents d'accéder à des pages présentant du contenu inapproprié ou préjudiciable. Le contrôle parental permet de bloquer des pages Web susceptibles de contenir du matériel potentiellement offensant. Les parents peuvent en outre interdire l'accès à 27 catégories de sites Web prédéfinies.

Les comptes d'utilisateur sont répertoriés dans la fenêtre **Contrôle parental** (**Configuration** > **Saisie des préférences de l'application...** > > **Contrôle parental**). Sélectionnez le compte à soumettre à un contrôle parental. Pour spécifier le niveau de protection du compte en question, cliquez sur le bouton **Configuration...**. Pour créer un compte, cliquez sur le bouton **Ajouter...**. Vous serez alors redirigé vers la fenêtre de comptes du système d'exploitation.

Dans la fenêtre **Configuration du contrôle parental**, sélectionnez un des profils prédéfinis dans le menu déroulant **Profil de configuration** ou copiez la configuration de contrôle parental d'un autre compte. Chaque profil contient une liste modifiée des catégories autorisées. Lorsqu'une catégorie est cochée, elle est autorisée. Placez le pointeur de la souris sur une catégorie pour afficher une liste de pages Web relevant de cette catégorie.

Pour modifier la liste des **pages Web autorisées et bloquées**, cliquez sur le bouton **Configuration...** dans le bas d'une fenêtre et ajoutez un nom de domaine à la liste voulue. Ne tapez pas *http://*. Il n'est pas nécessaire d'utiliser des caractères génériques (*). Si vous tapez simplement un nom de domaine, tous ses sous-domaines seront inclus. Par exemple, si vous ajoutez *google.com* à la **liste des pages Web autorisées**, tous les sous-domaines (*mail.google.com*, *news.google.com*, *maps.google.com* etc.) seront autorisés.

REMARQUE : Le blocage ou l'autorisation d'une page Web spécifique peut être plus précis que le blocage ou l'autorisation d'une catégorie de pages Web.

10. Mettre à jour

Des mises à jour régulières de ESET Cyber Security Pro sont nécessaires pour conserver le niveau maximum de sécurité. Le module de mise à jour garantit que le programme est toujours à jour en téléchargeant la dernière version de la base de signatures de virus.

En cliquant sur **Mettre à jour** dans le menu principal, vous pouvez connaître l'état actuel de la mise à jour, notamment la date et l'heure de la dernière mise à jour. Vous pouvez également savoir si une mise à jour est nécessaire. Pour démarrer manuellement la mise à jour, cliquez sur **Mettre à jour la base de signatures de virus**.

Dans des circonstances normales, lorsque les mises à jour sont téléchargées correctement, le message **La base de signatures de virus est à jour** s'affiche dans la fenêtre Mettre à jour. Si la base de signatures de virus ne peut pas être mise à jour, il est recommandé de vérifier les paramètres de mise à jour 17. Cette erreur est généralement liée à la saisie incorrecte de données d'authentification (nom d'utilisateur et mot de passe) ou à la configuration incorrecte des paramètres de connexion 23.

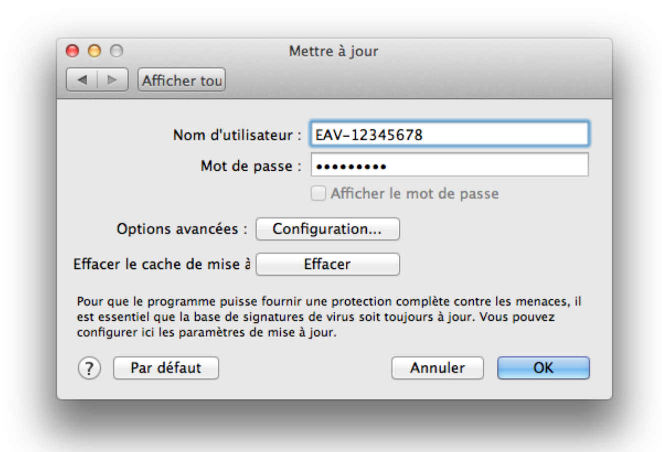
La fenêtre Mettre à jour contient également la version de la base de signatures de virus. Cette indication numérique est un lien actif vers le site Web d'ESET qui répertorie toutes les signatures ajoutées dans cette mise à jour.

REMARQUE : Votre nom d'utilisateur et votre mot de passe vous sont fournis par ESET après l'achat de ESET Cyber Security Pro.

10.1 Configuration des mises à jour

L'authentification du serveur de mise à jour est basée sur le nom d'utilisateur et le mot de passe générés qui vous ont été envoyés après l'achat.

Pour activer l'utilisation du mode test (téléchargement des mises à jour des versions précommerciales), cliquez sur le bouton **Configuration** > **Saisie des préférences de l'application...** (ou appuyez sur *cmd-,*) > **Mettre à jour**, cliquez sur le bouton **Configuration...** situé en regard de l'option **Options avancées** et cochez ensuite la case **Activer le mode test**.



Pour désactiver l'affichage des notifications dans la partie système de la barre d'état après chaque mise à jour, cochez la case **Ne pas afficher de notification de réussite de la mise à jour**.

Pour supprimer toutes les données de mise à jour stockées temporairement, cliquez sur le bouton **Effacer** situé en regard de l'option **Effacer le cache de mise à jour**. Utilisez cette option si vous rencontrez des problèmes de mise à jour.

10.2 Comment créer des tâches de mise à jour

Vous pouvez déclencher les mises à jour manuellement en cliquant sur **Mettre à jour la base de signatures de virus** dans la fenêtre principale qui s'affiche lorsque vous cliquez sur **Mettre à jour** dans le menu principal.

Les mises à jour peuvent également être exécutées sous forme de tâches planifiées. Pour configurer une tâche planifiée, cliquez sur **Outils** > **Planificateur**. Par défaut, les tâches suivantes sont activées dans ESET Cyber Security Pro :

- **Mise à jour automatique régulière**
- **Mise à jour automatique après ouverture de session utilisateur**

Chacune des tâches de mise à jour peut être modifiée selon les besoins de l'utilisateur. Outre les tâches de mise à jour par défaut, vous pouvez créer de nouvelles tâches avec votre propre configuration. Pour plus d'informations sur la création et la configuration des tâches de mise à jour, reportez-vous à la section Planificateur 18.

10.3 Mise à jour de ESET Cyber Security Pro vers une nouvelle version

Pour bénéficier d'une protection maximale, il est important d'utiliser la dernière version de ESET Cyber Security Pro. Pour rechercher une nouvelle version, cliquez sur **Accueil** dans le menu principal situé à gauche. Si une nouvelle version est disponible, un message s'affiche. Cliquez sur **En savoir plus...** pour afficher une nouvelle fenêtre contenant le numéro de la nouvelle version et la liste des modifications.

Cliquez sur **Oui** pour télécharger la dernière version ou cliquez sur **Pas maintenant** pour fermer la fenêtre et télécharger la mise à niveau ultérieurement.

Si vous avez cliqué sur **Oui**, le fichier est téléchargé dans le dossier des téléchargements (ou dans le dossier par défaut défini par votre navigateur). Lorsque le téléchargement du fichier est terminé, lancez le fichier et suivez les instructions d'installation. Votre nom d'utilisateur et votre mot de passe sont transférés automatiquement vers la nouvelle installation. Il est recommandé de vérifier régulièrement si des mises à niveau sont disponibles, en particulier si vous installez ESET Cyber Security Pro à partir d'un CD ou d'un DVD.

11. Outils

Le menu **Outils** contient des modules qui simplifient l'administration du programme et offrent des options supplémentaires pour les utilisateurs chevronnés.

11.1 Fichiers journaux

Les fichiers journaux contiennent tous les événements importants qui se sont produits et fournissent un aperçu des menaces détectées. La consignation (enregistrement dans les fichiers journaux) représente un puissant outil pour l'analyse système, la détection de menaces et le dépannage. La consignation est toujours active en arrière-plan sans

interaction de l'utilisateur. Les informations sont enregistrées en fonction des paramètres de verbosité actifs. Il est possible de consulter les messages texte et les journaux, ainsi que d'archiver les journaux, directement à partir de l'environnement ESET Cyber Security Pro.

Vous pouvez accéder aux fichiers journaux depuis le menu principal ESET Cyber Security Pro en cliquant sur **Outils** > **Journaux**. Sélectionnez le type de journal souhaité dans le menu déroulant **Journal**, en haut de la fenêtre. Les journaux suivants sont disponibles :

1. **Menaces détectées** : cette option permet de consulter toutes les informations concernant les événements liés à la détection d'infiltrations.
2. **Événements** : cette option permet aux administrateurs système et aux utilisateurs de résoudre des problèmes. Toutes les actions importantes exécutées par ESET Cyber Security Pro sont enregistrées dans les journaux des événements.
3. **Analyse de l'ordinateur** : cette fenêtre affiche toutes les analyses effectuées. Pour afficher les détails d'une analyse de l'ordinateur à la demande, double-cliquez sur l'entrée correspondante.
4. **Parental** : liste de toutes les pages Web bloquées par le contrôle parental.
5. **Pare-feu** : résultats de tous les événements liés au réseau.

Vous pouvez copier les informations affichées dans chaque section directement dans le Presse-papiers en sélectionnant l'entrée souhaitée, puis en cliquant sur le bouton **Copier**.

11.1.1 Maintenance des journaux

La configuration de la consignation de ESET Cyber Security Pro est accessible à partir de la fenêtre principale du programme. Cliquez sur **Configuration** > **Saisie des préférences de l'application...** (ou appuyez sur *cmd-,*) > **Fichiers journaux**. Les options suivantes peuvent être spécifiées pour les fichiers journaux :

- **Supprimer les anciennes entrées du journal automatiquement** : les entrées de journal plus anciennes que le nombre de jours spécifié sont automatiquement supprimées.
- **Optimiser automatiquement les fichiers journaux** : permet la défragmentation des fichiers journaux si le pourcentage spécifié d'enregistrements inutilisés est dépassé.

Pour configurer l'option **Filtre par défaut des entrées du journal**, cliquez sur le bouton **Modifier** et sélectionnez/désélectionnez les types de journaux en fonction de vos besoins.

11.1.2 Filtrage des journaux

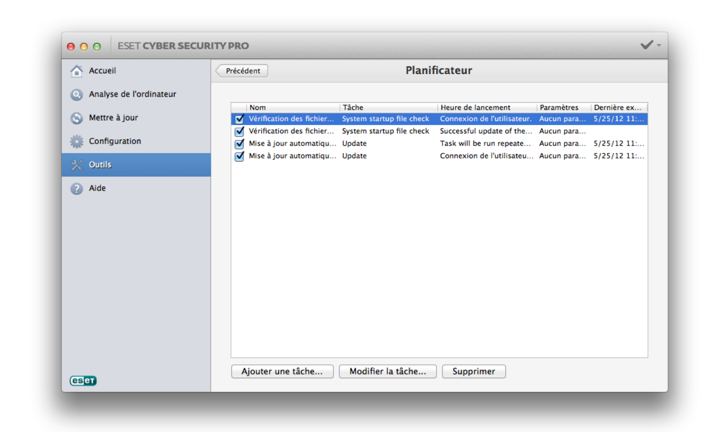
Les journaux stockent des informations sur les événements système importants : La fonctionnalité de filtrage des journaux permet d'afficher des entrées concernant un type d'événement spécifique.

Les types de journaux les plus fréquemment utilisés sont répertoriés ci-dessous :

- **Avertissements critiques** : erreurs système critiques (par exemple, le démarrage de la protection antivirus a échoué).
- **Erreurs** : messages d'erreur du type *Erreur de téléchargement de fichier* et erreurs critiques.
- **Avertissements** : messages d'avertissement.
- **Entrées informatives** : messages d'informations concernant des mises à jour, des alertes, etc.
- **Entrées de diagnostic** : informations nécessaires au réglage du programme et de toutes les entrées décrites ci-dessus.

11.2 Planificateur

Le **planificateur** est accessible depuis le menu principal de ESET Cyber Security Pro, dans **Outils**. Le **planificateur** contient la liste de toutes les tâches planifiées et des propriétés de configuration telles que la date et l'heure prédéfinies, ainsi que le profil d'analyse utilisé.



Le planificateur gère et lance les tâches planifiées qui ont été préalablement définies et configurées. La configuration et les propriétés comprennent des informations telles que la date et l'heure, ainsi que des profils spécifiques à utiliser pendant l'exécution de ces tâches.

Par défaut, les tâches planifiées suivantes sont affichées dans le planificateur :

- Maintenance des journaux (une fois que l'option **Afficher les tâches système** est activée dans la configuration du planificateur)
- Vérification des fichiers de démarrage après ouverture de session utilisateur
- Vérification des fichiers de démarrage après mise à jour réussie de la base de signatures de virus

- Mise à jour automatique régulière
- Mise à jour automatique après ouverture de session utilisateur

Pour modifier la configuration d'une tâche planifiée existante (par défaut ou définie par l'utilisateur), appuyez sur la touche Ctrl, cliquez sur la tâche à modifier et sélectionnez **Modifier...**. Vous pouvez également sélectionner la tâche et cliquer sur le bouton **Modifier la tâche...**

11.2.1 Création de nouvelles tâches

Pour créer une nouvelle tâche dans le planificateur, cliquez sur le bouton **Ajouter une tâche...** ou appuyez sur la touche Ctrl, cliquez dans le champ vierge et sélectionnez **Ajouter...** dans le menu contextuel. Cinq types de tâches planifiées sont disponibles :

- **Exécuter l'application**
- **Mettre à jour**
- **Maintenance des journaux**
- **Analyse de l'ordinateur à la demande**
- **Vérification des fichiers de démarrage du système**

La tâche planifiée la plus fréquente étant la mise à jour, nous allons expliquer comment ajouter une nouvelle tâche de mise à jour.

Dans le menu déroulant **Tâche planifiée**, sélectionnez **Mettre à jour**. Saisissez le nom de la tâche dans le champ **Nom de la tâche**. Sélectionnez la fréquence de la tâche dans le menu déroulant **Exécuter la tâche**. Selon la fréquence sélectionnée, vous êtes invité à choisir différents paramètres de mise à jour.

Si vous sélectionnez **Définie par l'utilisateur**, le système vous invite à indiquer la date et l'heure au format cron (pour plus d'informations, reportez-vous à la section Création d'une tâche définie par l'utilisateur 19).

À l'étape suivante, définissez l'action à entreprendre si la tâche ne peut pas être effectuée ou terminée à l'heure planifiée. Les trois options suivantes sont disponibles :

- **Patienter jusqu'à la prochaine heure planifiée**
- **Exécuter la tâche dès que possible**
- **Exécuter la tâche immédiatement si le temps écoulé depuis la dernière exécution dépasse l'intervalle spécifié** (l'intervalle peut être défini à l'aide de l'option **Intervalle minimal entre deux tâches**)

Dans l'étape suivante, une fenêtre récapitulative apparaît ; elle affiche des informations sur la tâche planifiée en cours. Cliquez sur le bouton **Terminer**.

La nouvelle tâche planifiée est ajoutée à la liste des tâches planifiées.

Par défaut, le système contient les tâches planifiées essentielles qui garantissent le fonctionnement correct du produit. Ces tâches ne doivent pas être modifiées et sont masquées par défaut. Pour modifier cette option et afficher ces tâches, sélectionnez **Configuration** > **Saisie des préférences de l'application...** (ou appuyez sur `cmd-,`) > **Planificateur** et sélectionnez l'option **Afficher les tâches système**.

11.2.2 Création d'une tâche définie par l'utilisateur

La date et l'heure de la tâche **Définie par l'utilisateur** doivent être indiquées au format cron sur l'année (chaîne composée de 6 champs séparés par un espace vierge) :
`minute(0-59) heure(0-23) jour du mois(1-31) mois(1-12) année(1970-2099) jour de la semaine(0-7)(dimanche = 0 ou 7)`

Exemple :
`30 6 22 3 2012 4`

Caractères spéciaux pris en charge dans les expressions cron :
- astérisque (`*`) - l'expression correspond à toutes les valeurs du champ ; par exemple, un astérisque dans le 3e champ (jour du mois) signifie « tous les jours »
- tiret (`-`) - définit des plages ; par exemple, `3-9`
- virgule (`,`) - sépare les éléments d'une liste ; par exemple, `1,3,7,8`
- barre oblique (`/`) - définit des incréments de plages ; par exemple, `3-28/5` dans le 3e champ (jour du mois) indique le 3e jour du mois, puis une fréquence tous les 5 jours.

Les noms de jour (Monday-Sunday) et de mois (January-December) ne sont pas pris en charge.

REMARQUE : si vous définissez un jour du mois et un jour de la semaine, la commande n'est exécutée que si les deux champs correspondent.

11.3 Quarantaine

La principale fonction de la quarantaine consiste à stocker les fichiers infectés en toute sécurité. Les fichiers doivent être placés en quarantaine s'ils ne peuvent pas être nettoyés, s'il est risqué ou déconseillé de les supprimer ou s'ils sont détectés erronément par ESET Cyber Security Pro.

Vous pouvez choisir de mettre n'importe quel fichier en quarantaine. Cette action est conseillée si un fichier se comporte de façon suspecte mais n'a pas été détecté par l'analyseur antivirus. Les fichiers mis en quarantaine peuvent être soumis pour analyse au Laboratoire de menaces ESET.

Les fichiers du dossier de quarantaine sont répertoriés dans un tableau qui affiche la date et l'heure de mise en quarantaine, le chemin de l'emplacement d'origine du fichier infecté, sa taille en octets, la raison (par exemple « ajouté par l'utilisateur ») et le nombre de menaces (par exemple, s'il s'agit d'une archive contenant plusieurs infiltrations). Le dossier de quarantaine dans lequel sont stockés les fichiers en quarantaine (*/Library/Application Support/Eset/esets/cache/quarantine*) reste dans le système même après la désinstallation de ESET Cyber Security Pro. Les fichiers en quarantaine sont stockés en toute sécurité dans un format crypté et peuvent être restaurés après l'installation de ESET Cyber Security Pro.

11.3.1 Mise en quarantaine de fichiers

ESET Cyber Security Pro met automatiquement en quarantaine les fichiers supprimés (si vous n'avez pas annulé cette option dans la fenêtre d'alerte). Au besoin, vous pouvez mettre manuellement en quarantaine tout fichier suspect en cliquant sur le bouton **Quarantaine...** Il est également possible d'utiliser le menu contextuel : appuyez sur la touche CTRL, cliquez dans le champ vierge, sélectionnez **Quarantaine**, choisissez le fichier à mettre en quarantaine et cliquez sur le bouton **Ouvrir**.

11.3.2 Restauration depuis la quarantaine

Les fichiers mis en quarantaine peuvent également être restaurés à leur emplacement d'origine. Utilisez pour cela le bouton **Restaurer** ; la fonction de restauration est également disponible dans le menu contextuel : appuyez sur la touche CTRL, cliquez sur le fichier à restaurer dans la fenêtre Quarantaine, puis cliquez sur **Restaurer**. Le menu contextuel propose également l'option **Restaurer vers...** qui permet de restaurer des fichiers vers un emplacement autre que celui d'origine dont ils ont été supprimés.

11.3.3 Soumission de fichiers de quarantaine

Si vous avez placé en quarantaine un fichier suspect non détecté par le programme ou si un fichier a été considéré par erreur comme étant infecté (par l'analyse heuristique du code par exemple) et placé en quarantaine, envoyez ce fichier au Laboratoire de menaces ESET. Pour soumettre un fichier mis en quarantaine, appuyez sur CTRL, cliquez sur le fichier et sélectionnez **Soumettre le fichier pour analyse** dans le menu contextuel.

11.4 Processus en cours

La liste **Processus en cours** affiche les processus en cours d'exécution sur l'ordinateur. ESET Cyber Security Pro fournit des informations détaillées sur les processus en cours pour protéger les utilisateurs à l'aide de la technologie ESET Live Grid.

- **Processus** : nom du processus en cours d'exécution sur l'ordinateur. Pour afficher tous les processus en cours, il est également possible d'utiliser Activity Monitor (dans */Applications/Utilities*).
- **Niveau de risque** : dans la majorité des cas, ESET Cyber Security Pro et la technologie ESET Live Grid attribuent des niveaux de risque aux objets (fichiers, processus, etc.) sur la base d'une série de règles heuristiques qui examinent les caractéristiques de chaque objet, puis évaluent le potentiel d'activité malveillante. Cette analyse heuristique attribue aux objets un niveau de risque. Les applications connues marquées en vert sont saines (répertoriées dans la liste blanche) et sont exclues de l'analyse. Cela permet d'accroître la rapidité des analyses à la demande et en temps réel. Une application marquée comme étant inconnue (jaune) n'est pas nécessairement un logiciel malveillant. Il s'agit généralement d'une nouvelle application. Si un fichier vous semble suspect, vous pouvez le soumettre pour analyse au laboratoire de recherche sur les menaces d'ESET. Si le fichier s'avère être une application malveillante, sa détection sera ajoutée à l'une des prochaines mises à jour.
- **Nombre d'utilisateurs** : nombre d'utilisateurs utilisant une application donnée. Ces informations sont collectées par la technologie ESET Live Grid.
- **Temps de découverte** : durée écoulée depuis la détection de l'application par la technologie ESET Live Grid.
- **ID du progiciel** : nom du fournisseur ou du processus de l'application.

Lorsque vous cliquez sur un processus, les informations suivantes apparaissent dans la partie inférieure de la fenêtre :

- **Fichier** : emplacement de l'application sur l'ordinateur,
- **Taille du fichier** : taille physique du fichier sur le disque,
- **Description du fichier** : caractéristiques du fichier basées sur la description émanant du système d'exploitation,
- **ID du progiciel** : nom du fournisseur ou du processus de l'application,
- **Version du fichier** : informations fournies par l'éditeur de l'application,
- **Nom du produit** : nom de l'application et/ou nom de l'entreprise.

11.5 Live Grid

Le système d'alerte anticipée Live Grid veille à ce qu'ESET soit immédiatement et continuellement informé des nouvelles infiltrations. Ce système bidirectionnel remplit un seul objectif : améliorer la protection que nous vous offrons. La meilleure façon de veiller à ce que nous détections les nouvelles menaces dès qu'elles apparaissent est de nous relier au plus grand nombre possible de nos clients et de les utiliser comme « éclaireurs ». Deux options sont possibles :

1. Vous pouvez décider de ne pas activer le système d'alerte anticipée Live Grid. Vous ne perdrez aucune fonctionnalité du logiciel et continuerez de recevoir la meilleure protection que nous offrons.
2. Vous pouvez configurer le système d'alerte anticipée Live Grid afin de nous soumettre des informations anonymes sur les nouvelles menaces et l'emplacement du nouveau code menaçant. Ce fichier peut être envoyé à ESET pour une analyse détaillée. L'étude de ces menaces aidera ESET à mettre à jour sa base de données de menaces et à améliorer la capacité du programme à détecter les menaces.

Le système d'alerte anticipée Live Grid collecte des informations sur votre ordinateur concernant des menaces nouvellement détectées. Ces informations peuvent contenir un exemple ou une copie du fichier dans lequel la menace est apparue, le chemin d'accès à ce fichier, le nom du fichier, la date et l'heure, le processus qui a permis l'apparition de la menace sur votre ordinateur et des informations sur le système d'exploitation de votre ordinateur.

Bien qu'il se puisse que ce processus dévoile occasionnellement au Laboratoire de menaces ESET certaines informations sur vous ou votre ordinateur (noms d'utilisateur dans un chemin de répertoires, etc.), ces informations ne seront utilisées à AUCUNE autre fin que celle de nous permettre de réagir immédiatement aux nouvelles menaces.

La configuration de Live Grid est accessible à partir de la section **Configuration** > **Saisie des préférences de l'application...** (ou appuyez sur *cmd-,*) > **Live Grid**. Sélectionnez l'option **Activer le système d'alerte anticipé Live Grid** pour l'activer, puis cliquez sur le bouton **Configuration...** en regard de l'intitulé **Options avancées**.

11.5.1 Configuration de Live Grid

Par défaut, ESET Cyber Security Pro est configuré pour soumettre les fichiers suspects au laboratoire de recherche sur les menaces d'ESET pour obtenir une analyse détaillée. Si vous ne souhaitez pas soumettre ces fichiers automatiquement, désélectionnez l'option **Soumission des fichiers suspects**.

Si vous trouvez un fichier suspect, vous pouvez le soumettre à notre laboratoire de recherche sur les menaces pour analyse. Pour cela, cliquez sur **Outils** > **Soumettre le fichier pour analyse** à partir de la fenêtre du programme principal. S'il s'agit d'une application malveillante, sa détection sera ajoutée à la prochaine mise à jour de la base des signatures de virus.

Soumission des informations statistiques anonymes : le système d'avertissement anticipé ESET Live Grid collecte des informations anonymes sur votre ordinateur concernant des menaces nouvellement détectées. Ces informations incluent le nom de l'infiltration, la date et l'heure de détection, la version du produit de sécurité ESET, ainsi que des informations sur la version du système d'exploitation de votre ordinateur et ses paramètres régionaux. Les statistiques sont généralement envoyées aux serveurs ESET une ou deux fois par jour.

Voici un exemple de statistiques soumises :

```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=9.5.0
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=Users/UserOne/Documents/Incoming/rdgFR1463
[1].zip
```

Filtre d'exclusion : cette option permet d'exclure certains types de fichiers de la soumission. Par exemple, il peut être utile d'exclure des fichiers qui peuvent comporter des informations confidentielles, tels que des documents ou des feuilles de calcul. Les fichiers les plus ordinaires sont exclus par défaut (.doc, .rtf, etc.). Vous pouvez ajouter des types de fichiers à la liste des fichiers exclus.

Email de la personne à contacter (facultatif) : votre adresse électronique est utilisée si l'analyse exige des informations complémentaires. Notez que vous ne recevrez pas de réponse d'ESET, à moins que des informations complémentaires soient nécessaires.

12. Interface utilisateur

Les options de la configuration de l'interface utilisateur permettent d'adapter l'environnement de travail selon vos besoins. Ces options sont accessibles depuis la section **Configuration** > **Saisie des préférences de l'application...** (ou appuyez sur *cmd-,*) > **Interface**.

Pour activer l'écran d'accueil de ESET Cyber Security Pro au démarrage du système, sélectionnez l'option **Afficher l'écran de démarrage**.

L'option **Application présente dans le Dock** permet d'afficher l'icône de ESET Cyber Security Pro dans le Dock de Mac OS et de basculer entre ESET Cyber Security Pro et d'autres applications actives en appuyant sur *cmd-tab*. Les modifications entrent en vigueur après le redémarrage de ESET Cyber Security Pro (généralement provoqué par un redémarrage de l'ordinateur).

L'option **Utiliser le menu standard** permet d'utiliser certains raccourcis clavier (voir Raccourcis clavier 6) et d'afficher certains éléments du menu standard (interface utilisateur, Configuration et Outils) sur la barre de menu Mac OS (en haut de l'écran).

Pour activer les info-bulles pour certaines options de ESET Cyber Security Pro, sélectionnez l'option **Afficher les info-bulles**.

L'option **Afficher les fichiers masqués** vous permet d'afficher et de sélectionner les fichiers masqués dans la configuration des **cibles à analyser** d'une **analyse de l'ordinateur**.

12.1 Alertes et notifications

La section **Alertes et notifications** vous permet de configurer le mode de traitement des alertes en cas de menace et des notifications système dans ESET Cyber Security Pro.

La désactivation de l'option **Afficher les alertes** annule toutes les fenêtres d'alerte et n'est adaptée qu'à des situations très précises. Nous recommandons à la majorité des utilisateurs de conserver l'option par défaut (activée).

La sélection de l'option **Afficher les notifications sur le Bureau** active l'affichage des fenêtres d'alerte sur le bureau (par défaut dans l'angle supérieur droit de votre écran) sans aucune intervention de l'utilisateur. Vous pouvez définir la période pendant laquelle une notification est affichée en réglant la valeur **Fermer automatiquement les notifications après** X **secondes**.

Pour afficher uniquement les notifications nécessitant une interaction de l'utilisateur lors de l'exécution d'applications en mode plein écran, activez l'option **Activer le mode plein écran** . Cette option est utile lorsque vous utilisez des présentations ou effectuez toute autre opération nécessitant l'intégralité de l'écran.

12.1.1 Configuration avancée des alertes et notifications

ESET Cyber Security Pro affiche des boîtes d'alerte vous informant de la disponibilité d'une nouvelle version du programme, d'une mise à jour du système d'exploitation, de la désactivation de certains composants du programme, de la suppression de journaux, etc. Vous pouvez éviter l'affichage de chaque notification en sélectionnant l'option **Ne plus afficher cette boîte de dialogue** dans le dialogue correspondant.

Liste des boîtes de dialogue (**Configuration** > **Saisie des préférences de l'application...** > **Alertes et notifications** > **Configuration...**) affiche la liste de toutes les boîtes d'alerte déclenchées par ESET Cyber Security Pro. Pour activer ou masquer chaque notification, activez la case à gauche du **nom de la notification**. Vous pouvez aussi définir des **conditions d'affichage** des notifications sur les nouvelles versions du programme et du système d'exploitation.

12.2 Privilèges

Les paramètres ESET Cyber Security Pro peuvent être très importants pour la stratégie de sécurité de votre organisation. Des modifications non autorisées peuvent mettre en danger la stabilité et la protection de votre système. Par conséquent, vous pouvez choisir les utilisateurs qui sont autorisés à modifier la configuration du programme.

Pour définir les utilisateurs privilégiés, cliquez sur **Configuration** > **Saisie des préférences de l'application...** (ou appuyez sur *cmd-,*) > **Privilèges**.

Il est essentiel que le programme soit correctement configuré pour garantir le maximum de sécurité au système. Tout changement non autorisé peut provoquer la perte de données importantes. Pour définir la liste des utilisateurs privilégiés, il vous suffit de sélectionner les utilisateurs dans la liste **Utilisateurs** dans la partie gauche et de cliquer sur le bouton **Ajouter**. Pour afficher tous les utilisateurs du système, sélectionnez l'option **Afficher tous les utilisateurs**. Pour supprimer un utilisateur, sélectionnez son nom dans la liste **Utilisateurs privilégiés** située à droite, puis cliquez sur **Supprimer**.

REMARQUE : si la liste des utilisateurs privilégiés est vide, tous les utilisateurs du système sont autorisés à modifier les paramètres du programme.

12.3 Menu contextuel

L'intégration des menus contextuels peut être activée dans la section **Configuration** > **Saisie des préférences de l'application...** (ou appuyez sur *cmd-,*) > **Menu contextuel** en sélectionnant l'option **Intégrer dans le menu contextuel**. Vous devez vous déconnecter ou redémarrer l'ordinateur pour que les modifications entrent en vigueur. Les options du menu contextuel sont disponibles dans la fenêtre du **Finder** lorsque vous appuyez sur le bouton ctrl en cliquant sur n'importe quel fichier.

13. Divers

13.1 Importer et exporter les paramètres

L'importation et l'exportation des configurations de ESET Cyber Security Pro sont disponibles dans le volet **Configuration**.

Les opérations d'importation et d'exportation utilisent des fichiers d'archive pour stocker la configuration. Ces opérations sont utiles si vous devez sauvegarder la configuration actuelle de ESET Cyber Security Pro pour l'utiliser ultérieurement. L'option Exporter les paramètres est également pratique pour les utilisateurs qui souhaitent utiliser leur configuration ESET Cyber Security Pro préférée sur plusieurs systèmes. Il leur suffit d'importer le fichier de configuration pour transférer les paramètres souhaités.



13.1.1 Importer les paramètres

Pour importer une configuration, cliquez sur **Configuration** > **Importer et exporter les paramètres...** à partir du menu principal, puis sélectionnez l'option **Importer les paramètres**. Saisissez le nom du fichier de configuration ou cliquez sur le bouton **Parcourir...** pour accéder au fichier de configuration à importer.

13.1.2 Exporter les paramètres

Pour exporter une configuration, cliquez sur **Configuration** > **Importer et exporter les paramètres...** à partir du menu principal. Sélectionnez l'option **Exporter les paramètres** et entrez le nom du fichier de configuration. Utilisez le navigateur pour sélectionner un emplacement de votre ordinateur afin d'enregistrer le fichier de configuration.

13.2 Configuration du serveur proxy

Les paramètres de serveur proxy peuvent être configurés dans **Configuration** > **Saisie des préférences de l'application ....** (ou appuyez sur *cmd-,*) > **Serveur proxy**. La spécification du serveur proxy à ce niveau définit les paramètres de serveur proxy globaux pour toutes les fonctions de ESET Cyber Security Pro. Les paramètres définis ici seront utilisés par tous les modules nécessitant une connexion à Internet.

Pour spécifier des paramètres de serveur proxy à ce niveau, activez la case **Utiliser le serveur proxy**, puis entrez l'adresse IP ou l'URL du serveur proxy dans le champ **Serveur proxy**. Dans le champ **Port**, spécifiez le port sur lequel le serveur proxy accepte les connexions (3128 par défaut).

Si la communication avec le serveur proxy exige une authentification, cochez la case **Le serveur proxy exige une authentification** et entrez un **nom d'utilisateur** et un **mot de passe** valides dans les champs correspondants.

14. Glossaire

14.1 Types d'infiltrations

Une infiltration est un élément de logiciel malveillant qui tente de s'introduire dans l'ordinateur d'un utilisateur et/ou de l'endommager.

14.1.1 Virus

Un virus est une infiltration qui endommage les fichiers existants de votre ordinateur. Les virus informatiques sont comparables aux virus biologiques parce qu'ils utilisent des techniques similaires pour se propager d'un ordinateur à l'autre.

Les virus informatiques attaquent principalement les fichiers, scripts et documents exécutables. Pour proliférer, un virus attache son « corps » à la fin d'un fichier cible. En bref, un virus informatique fonctionne de la manière suivante : après l'exécution du fichier infecté, le virus s'active lui-même (avant l'application originale) et exécute sa tâche prédéfinie. C'est après seulement que l'application originale peut s'exécuter. Un virus ne peut pas infecter un ordinateur à moins qu'un utilisateur n'exécute ou n'ouvre lui-même le logiciel malveillant (accidentellement ou délibérément).

Les virus peuvent varier en fonction de leur gravité et de leur cible. Certains sont extrêmement dangereux parce qu'ils ont la capacité de supprimer délibérément des fichiers du disque dur. D'autres, en revanche, ne causent pas de réels dommages : ils ne servent qu'à gêner l'utilisateur et à démontrer les compétences techniques de leurs auteurs.

Il est important de noter que, contrairement aux chevaux de Troie et aux spyware, les virus sont de plus en plus rares, car d'un point de vue commercial, ils ne sont pas très attrayants pour les auteurs de logiciels malveillants. En outre, le terme « virus » est souvent utilisé mal à propos pour couvrir tout type d'infiltrations. On tend à le remplacer progressivement par le terme « logiciel malveillant » ou « malware » en anglais.

Si votre ordinateur est infecté par un virus, il est nécessaire de restaurer l'état original des fichiers infectés, c'est-à-dire de les nettoyer à l'aide d'un programme antivirus.

14.1.2 Vers

Un ver est un programme contenant un code malveillant qui attaque les ordinateurs hôtes et se propage via un réseau. La différence fondamentale entre les virus et les vers réside dans le fait que les vers ont la capacité de se répliquer et de voyager par eux-mêmes. Ils ne dépendent pas des fichiers hôtes (ou des secteurs d'amorçage). Les vers se propagent par l'intermédiaire d'adresses électroniques de votre liste de contacts ou exploitent les vulnérabilités de sécurité des applications réseau.

Les vers sont ainsi susceptibles de vivre beaucoup plus longtemps que les virus. Par le biais d'Internet, ils peuvent se propager à travers le monde en quelques heures seulement et parfois en quelques minutes. Leur capacité à se répliquer indépendamment et rapidement les rend plus dangereux que les autres types de logiciels malveillants.

Un ver activé dans un système peut être à l'origine de plusieurs dérèglements : il peut supprimer des fichiers, dégrader les performances du système ou même désactiver certains programmes. Par sa nature, il peut servir de « moyen de transport » à d'autres types d'infiltrations.

Si votre ordinateur est infecté par un ver, il est recommandé de supprimer les fichiers infectés, car ils contiennent probablement du code malveillant.

14.1.3 Chevaux de Troie

Les chevaux de Troie étaient auparavant définis comme une catégorie d'infiltrations ayant pour particularité de se présenter comme des programmes utiles pour duper ensuite les utilisateurs qui acceptent de les exécuter. Aujourd'hui, les chevaux de Troie n'ont plus besoin de se déguiser. Leur unique objectif est de trouver la manière la plus facile de s'infiltrer pour accomplir leurs desseins malveillants. Le terme « cheval de Troie » est donc devenu un terme très général qui décrit toute infiltration qui n'entre pas dans une catégorie spécifique.

La catégorie étant très vaste, elle est souvent divisée en plusieurs sous-catégories :

- Téléchargeur : logiciel malveillant qui est en mesure de télécharger d'autres infiltrations sur Internet.
- Dropper : type de cheval de Troie conçu pour déposer d'autres types de logiciels malveillants sur des ordinateurs infectés.
- Backdoor : application qui communique à distance avec les pirates et leur permet d'accéder à un système et d'en prendre le contrôle.
- Keylogger : programme qui enregistre chaque touche sur laquelle tape l'utilisateur et envoie les informations aux pirates.
- Composeur : programme destiné à se connecter à des numéros surtaxés. Il est presque impossible qu'un utilisateur remarque qu'une nouvelle connexion a été créée. Les composeurs ne peuvent porter préjudice qu'aux utilisateurs ayant des modems par ligne commutée, qui sont de moins en moins utilisés.
- Les chevaux de Troie prennent généralement la forme de fichiers exécutables. Si un fichier est identifié comme cheval de Troie sur votre ordinateur, il est recommandé de le supprimer, car il contient sans doute du code malveillant.

14.1.4 Rootkits

Les rootkits sont des programmes malveillants qui permettent aux attaquants via Internet d'accéder à un système tout en cachant leur présence. Après avoir accédé à un système (généralement en exploitant une vulnérabilité de celui-ci), les rootkits utilisent des fonctions du système d'exploitation pour éviter d'être détectés par les logiciels antivirus : ils cachent leurs processus et fichiers. Il est donc quasi impossible de les détecter par des techniques de test ordinaires.

La prévention des rootkits peut se faire à deux niveaux :

1. Lors de leur tentative d'accès au système. Ils ne sont pas encore présents et sont donc inactifs. La plupart des logiciels antivirus sont capables d'éliminer les rootkits à ce niveau (en supposant qu'ils détectent effectivement ces fichiers comme étant des fichiers infectés).
2. Lorsqu'ils sont à couvert des tests traditionnels.

14.1.5 Logiciels publicitaires

Le terme anglais « adware » désigne parfois les logiciels soutenus par la publicité. Les programmes qui affichent des publicités entrent donc dans cette catégorie. Les logiciels publicitaires ouvrent généralement une nouvelle fenêtre contextuelle automatiquement dans un navigateur Internet. Cette fenêtre contient de la publicité ou modifie la page d'accueil du navigateur. Ils sont généralement associés à des programmes gratuits et permettent aux développeurs de ces programmes de couvrir les frais de développement de leurs applications (souvent utiles).

Les logiciels publicitaires proprement dits ne sont pas dangereux, mais ils peuvent déranger les utilisateurs en affichant ces publicités. Le danger tient dans le fait qu'ils peuvent aussi avoir des fonctions d'espionnage (comme les spyware).

Si vous décidez d'utiliser un logiciel gratuit, soyez particulièrement attentif au programme d'installation. La plupart des programmes d'installation vous avertissent en effet qu'ils installent également un logiciel publicitaire. Souvent, vous pourrez désactiver cette installation supplémentaire et installer le programme sans logiciel publicitaire.

Certains programmes refusent de s'installer sans leur logiciel publicitaire ou voient leurs fonctionnalités limitées. Cela signifie que les logiciels publicitaires accèdent souvent au système de manière « légale », dans la mesure où les utilisateurs l'ont accepté. Dans ce cas, mieux vaut jouer la sécurité. Si un logiciel publicitaire est détecté sur votre ordinateur, il est préférable de le supprimer, car il est fort probable qu'il contienne du code malveillant.

14.1.6 Spyware

Cette catégorie englobe toutes les applications qui envoient des informations confidentielles sans le consentement des utilisateurs et à leur insu. Les spyware utilisent des fonctions de traçage pour envoyer diverses données statistiques telles que la liste des sites Web visités, les adresses électroniques de la liste de contacts de l'utilisateur ou la liste des touches du clavier utilisées.

Les auteurs de ces spyware affirment que ces techniques ont pour but d'en savoir plus sur les besoins et intérêts des utilisateurs afin de mieux cibler les offres publicitaires. Le problème est qu'il n'y a pas de distinction claire entre les applications utiles et les applications malveillantes, et que personne ne peut garantir que les informations récupérées ne sont pas utilisées à des fins frauduleuses. Les données récupérées par les spyware peuvent être des codes de sécurité, des codes secrets, des numéros de compte bancaire, etc. Les spyware sont souvent intégrés aux versions gratuites d'un programme dans le but de générer des gains ou d'inciter à l'achat du logiciel. Les utilisateurs sont souvent informés de la présence d'un spyware au cours de l'installation d'un programme qui vise à les inciter à acquérir la version payante qui en est dépourvue.

Parmi les produits logiciels gratuits bien connus qui contiennent des spyware, on trouve les applications clients de réseaux P2P (poste à poste). Spyfalcon ou Spy Sheriff (et beaucoup d'autres) appartiennent à une sous-catégorie spécifique de spyware : ils semblent être des programmes antispyware alors qu'ils sont en réalité eux-mêmes des spyware.

Si un fichier est détecté comme étant un spyware sur votre ordinateur, il est recommandé de le supprimer, car il existe une forte probabilité qu'il contienne du code malveillant.

14.1.7 Applications potentiellement dangereuses

Il existe de nombreux programmes authentiques qui permettent de simplifier l'administration des ordinateurs en réseau. Toutefois, s'ils tombent entre de mauvaises mains, ces programmes sont susceptibles d'être utilisés à des fins malveillantes. ESET Cyber Security Pro permet de détecter ces menaces.

Les applications potentiellement dangereuses rentrent dans une classification utilisée pour les logiciels commerciaux légitimes. Cette classification comprend les programmes d'accès à distance, les applications de résolution de mot de passe ou les keyloggers (programmes qui enregistrent chaque frappe au clavier de l'utilisateur).

Si vous découvrez qu'une application potentiellement dangereuse est présente et fonctionne sur votre ordinateur (sans que vous l'ayez installée), consultez l'administrateur réseau ou supprimez l'application.

14.1.8 Applications potentiellement indésirables

Les applications potentiellement indésirables ne sont pas nécessairement malveillantes, mais elles sont susceptibles d'affecter les performances de votre ordinateur. L'installation de ces applications nécessite généralement l'accord de l'utilisateur. Si elles sont présentes sur votre ordinateur, votre système se comporte différemment (par rapport à son état avant l'installation). Voici les changements les plus significatifs :

- affichage de nouvelles fenêtres ;
- activation et exécution de processus cachés ;
- augmentation des ressources système utilisées ;
- modification des résultats de recherche ;
- communication avec des serveurs distants.

14.2 Types d'attaques à distance

Les attaquants disposent de nombreuses techniques spéciales pour infiltrer des systèmes à distance. Ces techniques se divisent en plusieurs catégories.

14.2.1 Attaques par déni de service

Le déni de service (DoS) cherche à rendre un ordinateur ou un réseau indisponible pour ses utilisateurs. La communication entre les utilisateurs affectés est bloquée et ne peut plus fonctionner correctement. Les ordinateurs exposés à de telles attaques doivent généralement faire l'objet d'un redémarrage pour fonctionner à nouveau correctement.

Le plus souvent, les cibles sont des serveurs Web et le but est de les rendre indisponibles pendant un certain temps.

14.2.2 Empoisonnement du cache DNS

En empoisonnant le DNS (serveur de noms de domaine), les pirates peuvent faire croire au serveur DNS de n'importe quel ordinateur que les fausses données qu'ils fournissent sont légitimes et authentiques. Ces fausses informations sont mises en cache pendant un certain temps, permettant aux attaquants de réécrire les réponses DNS d'adresses IP. Les utilisateurs qui tentent d'accéder à des sites Web sur Internet téléchargeront alors des virus ou des vers informatiques au lieu du contenu d'origine.

14.2.3 Vers informatiques

Un ver est un programme contenant un code malveillant qui attaque les ordinateurs hôtes et se propage via un réseau. Il exploite les failles de sécurité de diverses applications. Avec Internet, ils peuvent se propager dans le monde entier en quelques heures. Parfois même en quelques minutes.

La plupart des vers informatiques (Sasser, SqlSlammer) peuvent être évités en utilisant les paramètres de sécurité par défaut du pare-feu ou en bloquant les ports non protégés et inutilisés. Il est également essentiel de mettre à jour le système d'exploitation avec les correctifs de sécurité les plus récents.

14.2.4 Balayage de ports

Le balayage de ports vise à déterminer quels ports de l'ordinateur sont ouverts sur un ordinateur hôte d'un réseau. Un analyseur de ports est un logiciel conçu pour détecter ces ports.

Un port d'ordinateur est un point virtuel qui traite les données entrantes et sortantes. Il est donc crucial du point de vue de la sécurité. Dans un grand réseau, les informations collectées par les analyseurs de ports peuvent aider à identifier des vulnérabilités potentielles. Cette utilisation est légitime.

Cependant, le balayage des ports est souvent utilisé par des pirates pour tenter de compromettre la sécurité du réseau. La première étape consiste à envoyer des paquets sur chaque port. Selon le type de réponse, il est possible de déterminer quels ports sont utilisés. Le balayage en lui-même est inoffensif, mais sachez que cette opération peut révéler des vulnérabilités potentielles et permettre à des attaquants de prendre le contrôle d'ordinateurs à distance.

Il est recommandé aux administrateurs de réseau de bloquer tous les ports inutilisés et de protéger ceux qui sont utilisés contre tout accès non autorisé.

14.2.5 Désynchronisation TCP

La désynchronisation TCP est une technique utilisée dans les attaques de piratage TCP. Elle est déclenchée par un processus qui associe aux paquets entrants un numéro séquentiel différent du numéro attendu. Ces paquets sont alors rejetés (ou enregistrés en mémoire tampon, s'ils se trouvent dans la fenêtre de communication active).

Dans cette technique, les deux extrémités de la communication rejettent des paquets reçus, ce qui permet aux attaquants de s'infiltrer et de fournir des paquets présentant le numéro séquentiel correct. Les attaquants peuvent même manipuler ou modifier la communication.

Les attaques par piratage TCP visent à interrompre les communications entre serveur et client, ou entre pairs. Elles peuvent souvent être évitées en utilisant une authentification pour chaque segment TCP. Il est également conseillé d'utiliser les configurations recommandées pour vos unités réseau.

14.2.6 Relais SMB

SMBRelay et SMBRelay2 sont des programmes spéciaux capables de mener des attaques contre des ordinateurs distants. Ces programmes tirent parti du protocole de partage de fichiers SMB (Server Message Block), qui tourne par dessus NetBIOS. Un utilisateur qui partage un dossier ou un répertoire sur un LAN utilise fort probablement ce protocole de partage de fichiers.

Au sein d'une communication en réseau local, les ordinateurs s'échangent des hachages de mots de passe.

SMBRelay reçoit une connexion sur les ports UDP 139 et 445, relaie les paquets échangés entre le client et le serveur, puis les modifie. Après la connexion et l'authentification, le client est déconnecté. SMBRelay crée alors une nouvelle adresse IP virtuelle. SMBRelay relaie la communication du protocole SMB à l'exception de la négociation et de l'authentification. Les attaquants à distance peuvent utiliser l'adresse IP tant que l'ordinateur client est connecté.

SMBRelay2 fonctionne selon le même principe que SMBRelay, si ce n'est qu'il utilise des noms NetBIOS plutôt que des adresses IP. Les deux programmes peuvent mener des attaques de type « man-in-the-middle ». Ces attaques permettent à leurs auteurs de lire, insérer et modifier les messages échangés entre deux points de communication à leur insu. Les ordinateurs exposés à de telles attaques s'arrêtent souvent de répondre ou redémarrent de manière inattendue.

Pour éviter ces attaques, nous recommandons d'utiliser des mots de passe ou des clés d'authentification.

14.2.7 Attaques par ICMP

ICMP (Internet Control Message Protocol) est un protocole Internet populaire et largement utilisé. Il est essentiellement utilisé par des ordinateurs en réseau pour envoyer divers messages d'erreur.

Les attaquants à distance tentent d'exploiter les faiblesses du protocole ICMP. Celui-ci est conçu pour une communication unidirectionnelle ne nécessitant aucune authentification. Cela permet aux attaquants de déclencher des attaques par déni de service ou d'autres attaques permettant à des utilisateurs non autorisés d'accéder aux paquets entrants et sortants.

Exemples types d'attaques ICMP : envoi massif de pings ou de messages ICMP_ECHO et attaques par rebond. Les ordinateurs exposés à une attaque ICMP sont sensiblement ralentis (pour toutes les applications utilisant Internet) et éprouvent de la difficulté à se connecter à Internet.

14.3 Courrier électronique

Le courrier électronique (e-mail) est une forme de communication moderne qui présente de nombreux avantages. Elle est souple, rapide et directe, et a joué un rôle crucial dans la prolifération d'Internet dans le début des années 1990.

Malheureusement, le large anonymat que permettent le courrier électronique et Internet laisse une voie ouverte à des activités illégales telles que le spam. Celui-ci couvre aussi bien des publicités non sollicitées que des canulars et la diffusion de logiciels malveillants. L'inconfort et le risque que cela représente pour vous sont aggravés par le fait que le coût d'envoi des spams est infime et que leurs auteurs disposent de nombreux outils pour se procurer des nouvelles adresses électroniques. Qui plus est, le volume et la diversité du spam rendent difficile sa régulation. Plus longtemps vous utilisez la même adresse électronique, plus elle risque d'aboutir dans la base de données d'un moteur de spam. Voici quelques conseils de prévention :

- Si possible, ne publiez pas votre adresse électronique sur Internet,
- ne donnez votre adresse électronique qu'à des personnes de confiance,
- dans la mesure du possible, n'utilisez pas des alias courants - plus votre alias est compliqué, plus il sera difficile à épier,
- ne répondez pas à des messages de spam déjà parvenus dans votre boîte de réception,
- soyez prudent lorsque vous complétez des formulaires sur Internet - méfiez-vous en particulier d'options telles *Oui, je souhaite recevoir des informations*,
- utilisez des adresses électroniques « spécialisées » - par exemple une pour le travail, une pour vos amis, etc.,
- changez d'adresse électronique de temps à autre,
- utilisez une solution de blocage de spam.

14.3.1 Publicités

La publicité sur Internet est une des formes de communication commerciale en plus forte croissance. Ses principaux avantages en termes de marketing sont ses coûts minimes et une communication très directe ; qui plus est, les messages sont diffusés quasi instantanément. Nombre d'entreprises recourent à des outils de marketing par courrier électronique pour s'assurer une communication efficace avec leurs clients et leurs prospects.

Ce type de publicité est légitime, car il peut être intéressant de recevoir des informations commerciales sur certains produits. Hélas, de nombreuses entreprises envoient des messages commerciaux non sollicités en masse. Elles franchissent alors la frontière entre la publicité par courrier électronique et le spam.

Le volume de messages non sollicités est devenu un réel problème et ne montre aucun signe de ralentissement. Leurs auteurs tentent souvent de cacher le spam sous les dehors de messages légitimes.

14.3.2 Canulars

Un canular est une information erronée diffusée sur Internet. Le courrier électronique et les outils de communication tels que Skype et ICQ en sont les vecteurs privilégiés. Le message en lui-même est souvent une plaisanterie ou une légende urbaine.

Les canulars relatifs à des virus informatiques visent à susciter la crainte, l'incertitude et le doute chez les destinataires, en tentant de leur faire croire qu'il existe un « virus indétectable » qui supprime des fichiers et récupère les mots de passe ou effectue d'autres opérations néfastes sur leur système.

Certains canulars opèrent par contagion, en poussant leurs destinataires à transférer le message à leurs contacts. Il existe des canulars sur les téléphones mobiles, des faux appels à l'aide, des prétendus transferts de fonds secrets venant de l'étranger, etc. Souvent, il est malaisé de déterminer l'intention de l'auteur du message.

Si vous recevez un message vous invitant à le transférer à tous vos contacts, il est bien possible qu'il s'agisse d'un canular. De nombreux sites sur Internet permettent d'en vérifier la légitimité. Avant de transférer un tel message, effectuez une recherche sur Internet pour vous assurer qu'il ne s'agit pas d'un canular.

14.3.3 Hameçonnage

Le hameçonnage (en anglais : phishing) définit une activité criminelle basée sur des techniques « d'ingénierie sociale » (consistant à manipuler des personnes pour leur soutirer des informations confidentielles). Son but est d'obtenir l'accès à des données sensibles telles que des numéros de compte bancaire, des codes PIN, etc.

Souvent, la technique consiste à se faire passer pour une personne ou une entreprise de confiance (p. ex. une institution financière, une société d'assurances). Le message électronique peut sembler authentique et contiendra des graphismes et du contenu pouvant provenir à l'origine de la source usurpée. Sous divers prétextes (vérification des données, opérations financières), vous serez invité à fournir certaines données personnelles telles qu'un numéro de compte bancaire ou un nom d'utilisateur et un mot de passe. Ces données, si vous les envoyez, pourront facilement être détournées et utilisées à mauvais escient.

Les banques, compagnies d'assurances et autres entreprises légitimes ne vous demanderont jamais des noms d'utilisateur et des mots de passe par le biais de messages non sollicités.

14.3.4 Identification du spam

D'une manière générale, plusieurs signes peuvent vous aider à identifier du spam (messages non sollicités) dans votre boîte aux lettres. Si un message répond au moins à quelques-uns des critères ci-dessous, ce sera probablement un spam.

- L'adresse de l'expéditeur n'appartient pas à un de vos contacts,
- on vous propose une somme d'argent importante, mais vous devez commencer par engager un petit montant,
- sous divers prétextes (vérification des données, opérations financières), vous serez invité à fournir certaines données personnelles telles qu'un numéro de compte bancaire ou un nom d'utilisateur et un mot de passe,
- le message est rédigé dans une langue étrangère,
- vous êtes invité à acheter un produit qui ne vous intéresse pas ; si vous décidez de l'acheter quand même, assurez-vous que l'expéditeur est un vendeur fiable (consultez le fabricant original du produit),
- certains mots sont mal orthographiés afin de contourner les filtres antispam (par exemple *vaigra* au lieu de *viagra*, etc.).